NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

802.16 OFDM RAPIDLY DEPLOYED NETWORK FOR NEAR-REAL-TIME COLLABORATION OF EXPERT SERVICES IN MARITIME SECURITY OPERATIONS

by

Chris Marvin

September 2005

Thesis Advisor:	Alex Bordetsky
Second Reader:	David Netzer

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704-0188*

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** September 2005	**3. REPORT TYPE AND DATES COVERED** Master's Thesis

4. TITLE AND SUBTITLE: 802.16 OFDM Rapidly Deployed Network For Near-real-time Collaboration Of Expert Services In Maritime Security Operations	**5. FUNDING NUMBERS**
6. AUTHOR Christopher Marvin	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited	**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

The world's shipping lanes are an area of intense focus in the Global War on Terror. Every day millions of tons of cargo are shipped though thousands of ports. Most cargo is the harmless however some ships carry the weapons and human operators of terrorist organizations. To prevent the spread of weapons and terror suspects on the sea lanes, the cargo, passengers and crew of theses vessels must be subject to scrutiny that is orders of magnitude greater than current efforts. The ability to rapidly extend a network and provide virtual expert services to VBSS boarding teams, is crucial to protecting the United States and it's allies from sea born terror attacks and infiltration.

This thesis examines through scenario based experimentation the methods for implementing near-real-time collaborative work spaces in a virtual environment able to support VBSS operation any where in the world limited only by network connectivity. The use of collaborative tools vastly increases the amount, type and accuracy of information that can be processed. Radiation detection or classification and biometric fusion are two hundreds of virtual collaborative sources that can be leveraged as a force multiplier and brings network centric warfare to the maritime security domain.

14. SUBJECT TERMS 15. Mesh, Orthogonal Frequency Division Multiplexing (OFDM), Groove Virtual Office, Situational Awareness Multi Agent System, Internet, Nodes, Wireless, IEEE 802.16, Peer to Peer relationships, Collaborative Environment, Common Operating Picture, Tactical Network Topology, Lawrence Livermore National Laboratory, Tactical Satellite, Ultra-Wideband, Expert Service Reach-back.	**15. NUMBER OF PAGES** 87
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UL

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution unlimited

802.16 OFDM RAPIDLY DEPLOYED NETWORK FOR NEAR-REAL-TIME COLLABORATION OF EXPERT SERVICES IN MARITIME SECURITY OPERATIONS

Christopher E. Marvin
Lieutenant, United States Navy
B.S., The Pennsylvania State University, 1996

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
September 2005

Author: Christopher E. Marvin

Approved by: Alex Bordetsky
Thesis Advisor

David Netzer
Second Reader

Dan Boger
Chairman, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The world's shipping lanes are an area of intense focus in the Global War on Terror. Every day millions of tons of cargo are shipped though thousands of ports. Most cargo is the harmless however some ships carry the weapons and human operators of terrorist organizations. To prevent the spread of weapons and terror suspects on the sea lanes, the cargo, passengers and crew of theses vessels must be subject to scrutiny that is orders of magnitude greater than current efforts. The ability to rapidly extend a network and provide virtual expert services to VBSS boarding teams, is crucial to protecting the United States and it's allies from sea born terror attacks and infiltration.

This thesis examines through scenario based experimentation the methods for implementing near-real-time collaborative work spaces in a virtual environment able to support VBSS operation any where in the world limited only by network connectivity. The use of collaborative tools vastly increases the amount, type and accuracy of information that can be processed. Radiation detection or classification and biometric fusion are two hundreds of virtual collaborative sources that can be leveraged as a force multiplier and brings network centric warfare to the maritime security domain.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

ACRONYMS AND ABBREVIATIONS

API – Application Program Interface
BPSK – Binary Phase Shift Keying
CENETIX – Center for Network Innovation and Experimentation
CG –Coast Guard
CGC – Coast Guard Cutter
CONOPS – Concept of Operations
COTS – Commercial Off the Shelf
CSMA/CD – Carrier Sense Multiple Access Collision Detect
CSMA/CA – Carrier Sense Multiple Access Collision Avoidance
DoD – Department of Defense
DSL – Digital Subscriber Loop
EAL – Evaluation Assurance Level
ELINT – Electronic Intelligence
FINEX – Finished with Exercise
FIPS – Federal Information Processing Standard
GDK – Groove Development Kit
GHz – Gigahertz
GPS – Global Positioning System
GUI – Graphical User Interface
GWOT – Global War On Terror
HUMINT – Human Intelligence
ID – Identification
IEEE – Institute of Electrical and Electronic Engineers
IP – Internet Protocol
ISI – Initial Safety Inspection
ISP – Internet Service Provider
IST – Innovative Survivability Technologies
IT – Information Technology
Kbps – Kilobits Per Second
LAN – Local Area Network
LLNL – Lawrence Livermore National Lab
LOS – Line-of-sight
MAC – Media Access Control
MHz – Megahertz
M/V – Motor Vessel
MILSAT – Military Satellite
Mbps – Megabits Per Second
MS – Microsoft
NIC – Network Interface Card
NOC – Network Operations Center
NPS- Naval Postgraduate School
OFDM – Orthogonal Frequency Division Multiplexing

OPCEN – Operations Center
QAM – Quadrative Amplitude Modulation
PC – Personal Computer
PDA – Personal Digital Assistant
PHY – Physical Layer
PTZ – Pan-Tilt-Zoom
QPSK – Quadrature Phase Key Shifting
RF – Radio Frequency
SA – Situational Awareness
SATCOM – Satellite Communication
SOC – Shore Operations Center
SMS – Short Messaging System
SNMP – Simple Network Management Protocol
SSTP – Simple Symmetric Transfer Protocol
STAN - Surveillance and Target Acquisition Network
TACSAT – Tactical Satellite
TCP – Transmit Control Protocol
TDMA – Time Division Multiple Access
TDD – Time Division Duplexing
TNT – Tactical Network Topology
TOC – Tactical Operations Center
TOI – Target of Interest
UAV – Unmanned Aerial Vehicle
UDP – User Datagram Protocol
UI – User Interface
USCGC – United States Coast Guard Cutter
USCS – United States Customs Service
UWB – Ultra-Wideband
VBSS – Visit Board Search and Seizure
VHF – Very High Frequency
VPN – Virtual Private Network
WAN – Wide Area Network
WiFi – Wireless Fidelity
WLAN – Wireless Local Area Network
WMAN – Wireless Metropolitan Area Network
WiMAX - Worldwide Interoperability for Microwave Access
WMD – Weapon of Mass Destruction
XML – Extensible Markup Language

ACKNOWLEDGMENTS

I would like to thank Alex Bordetsky, Dave Netzer, Eugene Bourakov, Kevin Jones, Marianna Verett and the host of other hard working dedicated individuals that make CENETIX and TNT a perpetual success. I feel lucky and humble to have been part of a program that successfully supports our nation and our brothers in arms everyday.

To my son Cody, You are too young to understand how a child changes your life. One day however, I hope you will understand why I say thank you for all the opportunities that you provide for me to leave my work and the larger world around all of us and focus on something truly wonderful like you.

To the NPS Rifle & Pistol Team and the Carmel Gun Club, I have enjoyed two years of great competition and comradeship. Our continuation of the American tradition of marksmanship is noble endeavor. I hope to see many of you on the range in the future.

Lastly to my friends and family, who over the years have supported and even helped shape me into the person I am today. I could not have accomplished everything that I have, or continue to work in the capacity that I do, without all that I have learned and all that you have given to me over the years.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. HISTORY

The use of Naval boardings to inspect, search, and if required seize cargo and crew has been employed in peace time as well as war by every Navy in the world. From their inception, the United States Navy and Coast Guard have used ship boardings to control illegal trade and protect the citizens of the United States from groups or individuals that attempt to smuggle goods or weapons into the country with the intent of harm. Boarding vessels to prevent unlawful commerce in arms, illegal or dangerous goods and transport of persons wanted by the law, has been a primary means of sea control and core competency exercised by the United States Navy and Coast Guard for nearly 230 years.

Today the Navy and Coast Guard are still heavily involved in boarding operations termed Visit, Board, Search and Seizure (VBSS) operations. These operations are conducted routinely numerous times each day all over the world. Typically VBSS operations in United States territorial water are conducted by the United States Coast Guard in the frame work of emigration, trade, and transportation law enforcement. The Navy's role in VBSS operations on the other hand, is in international waters or foreign territorial waters as an instrument of international policy. Examples of this are the enforcement of United Nations sanctions or direct action with reference to United States foreign policy or protection of Unites States citizens and property abroad.

My personal experience with VBSS operations stem from numerous boardings conducted in the Arabian Gulf between October 1999 and February 2000 in support of United Nations sanctions and the "Oil for Food Program" imposed on Iraq by the UN following Gulf War I. The second time I was involved in VBSS operations was supporting Coast Guard counter narcotics operations off the west coast of Mexico and Central America in early 2001.

The VBSS boardings I was involved in were conducted in typical fashion with an all Navy team in the case of the Arabian Gulf boardings, and a Coast Guard Legal detachment in the counter narcotic operations. Most boarding operations are initiated by

hailing the target vessel in question and having it come to all stop or go to a designated place of anchorage for the subsequent VBSS operation. In limited cases vessels may be boarded under the condition of what is know as a "noncompliant boarding" where the target vessel must be boarded by an armed team and taken by force. The end result of all successful boardings is the placement of a VBSS team on a secured vessel to search for illicit cargo, or personnel.

The command and control communications technology used in today's VBSS operations is essentially unchanged from boardings conducted over the past 50 years. The only direct link back to the mother ship in most cases is a low power, low band width, unencrypted voice radio. More recently the Navy has moved to somewhat better technology that uses integrated ship's communications antennas and transceivers for increased range however, the communication is still only a voice link. The transfer of important documentation such as crew manifests, ship information, cargo documentation and most recently biometrics gathering, is slow and tedious. Most information is relayed and hand scribed. Even this method is impossible in the case of documentation duplication or biometrics finger print cards. All voice transcribed information that is gathered must be subsequently resent in a second voice report on a MILSAT network, included in a separate Naval message report of the boarding and in some cases hard documentation such as biometric data, photo copies, video documentation, and still photography must be forwarded by mail to the end destination. The high latency and redundant parallel paths of the data transmission from VBSS operations is strikingly inefficient and ineffective in fully leveraging VBSS operations in the sea power superiority domain.

B. OBJECTIVES

The research conducted within this thesis is focused on how to best apply rapidly deployable networking technology to provide the benefits of collaboration, force multiplication, network centric warfare and expert service reach-back to the VBSS operational environment. The GWOT has placed new and increasingly complex demands on the amount, type, and latency of information captured during VBSS operations. In the past, visual inspection of cargo, documentation, and crew by boarding

teams was enough to discriminate, at a reasonable level confidence, the need for further action such as seizure of crew and cargo. This method of boarding worked well to hold illegal trafficking of arms and people on the sea lanes to a manageable level in specific areas. When combined with other means of influence such as targeted political pressure or trade sanctions, it was a best effort solution. The modern challenge for VBSS operations can no longer target specific regions or nations. The movement of terrorists and weapons is a borderless problem expanding the enforcement region to all the oceans of the world instead of targeted regions. The expansion of the VBSS operational environment from regional to global requires an order of magnitude or more increase in efficiency.

The challenge of the global war on terror is not to, detour but to stop terrorists and weapons of mass destruction (WMD) from reaching the United States or its allies. The means to accomplish this task are daunting. WMDs and terrorists probably do not outwardly advertise themselves as dangerous. The only way to ensure that movement of such people and weapons is stopped in many areas will be with a boarding and search frequency approaching 100 percent. In this case a much greater volume data of varying types and media formats must be quickly gathered, transmitted, processed and acted upon in a short time frame. The limited physical resources of personnel and equipment drive time to be the critical variable in ship boarding operations.

The data types and volume of information required to be captured by VBSS teams to effectively pursue the global war on terror (GWOT) have rapidly overtaken the capability of low bandwidth, purely voice network capability. The ability to capture and transmit alternate forms of data such as voice, video, electronic sensor, and biometrics data with low latency is crucial to mission success. A force multiplier must be put into effect to make up for the physical shortfalls. In order to be most effective VBSS, like other operations, must move to leverage network centric operations. The creation of a virtual boarding party of collaborative experts can be formed to augment a physical boarding party and increases efficiency.

.

C. RESEARCH QUESTIONS

1. Use of 802.16 High Speed Backhaul

Can a commercial-off-the-self technology such as 802.16 OFDM provide a potentially viable, economic, fast, reliable, and highly mobile broadband wireless network extension from mother ship to target vessel or land base? What is the feasibility and efficiency of employing 802.16 OFDM under VBSS mission constraints.

2. Expert Source Reach-back

What is the viability and benefit of utilizing near-real-time reach-back to expert source collaborative partners in assisting boarding teams to rapidly assess situational awareness of boarded vessels and the potential force multiplication effects of better situational awareness?

3. Rapidly Deployable Network Concept of Operations

Utilizing 802.16 OFDM, can a core concept of operations be developed and tested that leverages network centric warfare concepts to virtually augment VBSS operation in the maritime security domain?

D. SCOPE

1. Test Viability

Deploy and test in field experimentation the viability of a portable 802.16 OFDM wireless radio network providing back-haul and networked services for local and remote VBSS assets.

2. Examine Collaborative Benefits

Examine through operational employment, if the tactical network extended by 802.16 OFDM portable nodes can provide the range and data transfer rates required to leverage expert services reach-back, advanced remote sensor technology (radiation detection, biometrics, etc.)

3. Analysis of Requirements

Through experimentation lessons learned provide insight to baseline requirements for operationally deployable wireless broadband links to support VBSS operations.

E. METHODOLOGY

Utilizing the CENETIX test-bed, VPN reach-back to Lawrence Livermore National Laboratory and The National Biometric Fusion Center, an 802.16 OFDM network will be expanded to a suspect vessel (USCGC HAWKSBILL) to provide back-haul for text, voice, video, radiation detection, and biometrics data. In addition, expert service providers will be able to collaborate through the common operational picture provided by a shared workspace in the Groove Networks software package to assess and provide insight to data gathered from the crew or cargo during the VBSS mission.

F. THESIS ORGANIZATION

The thesis is organized in the following manner: Chapter I was the history, scope and methodology behind the thesis field experimentation. Chapter II will address the Center for Network Innovation and Experimentation (CENETIX) at The Naval Postgraduate School and our partners in collaborative research and experimentation. Chapter III provides details on the Tactical Network Topology (TNT) test-bed as well as an overview of the 802.16 wireless protocol, connectivity, link budget and remote rapidly deployable LAN infrastructure. Chapter IV looks exclusively at the Redline AN-50M concept device communications, power management, portability, and potential improvements for future models. Chapter V combines the knowledge of the field experimentation data and current perceived operational requirements of the Navy and Coast Guard to develop a concept of operations for field portable 802.16 OFDM and similar technology. Chapter VI details the field data and lessons learned from the TNT 05-3 proof of concept ship boarding experiment. In Chapter VII the TNT 05-4 scenario based field experiment is detailed. Finally Chapter VIII concludes with closing thoughts and recommended areas for future research.

THIS PAGE INTENTIONALLY LEFT BLANK

II STUDENT RESEARCH TEST-BED

A. CENETIX

The Center for Innovation and Experimentation (CENETIX) headed by Dr Alex Bordetsky is the evolutionary result of two years of research and experimentation that directly supports the operational requirements of the armed forces, Department of Homeland Security, state and local governments. At any given time there are approximately 20-25 masters thesis students and 5-8 doctoral students involved in CENETIX research. The majority of the research students are military officers coming to the Naval Postgraduate School from operational commands. The combination of operational knowledge and a strong base of academic research knowledge brought together by students and faculty combines to form a unique partnership that focuses on bringing cutting edge, network centric, collaborative technology to real world operations.

The physical environment of CENETIX currently has nodes that occupy land, sea (surface and subsurface), and air. The Tactical Network Topology (TNT) stretches for over 120 miles along the central California Coast from seven miles off-shore in Monterey Bay to the California National Guard base of Camp Roberts, north of Paso Robles (Figure 1). Connectivity is handled by an independent 802.16 OFDM wireless network link controlled and maintained by CENETIX with a 18 megabits per second throughput. Two network operation centers (NOCs), one in Camp Roberts, and one at The Naval Postgraduate School are maintained and operated by students and faculty for network command, control, experimentation and data capture. In addition to the two stationary NOCs, the TNT grid also has a mobile NOC known as the Light Reconnaissance Vehicle (LRV) (Figure 2). CENETIX and TNT have access to and operate various land, air, and sea manned and unmanned vehicles that integrate into the TNT network architecture and pass near-real-time situational awareness data into the NOCs and through VPN to experimental partners.

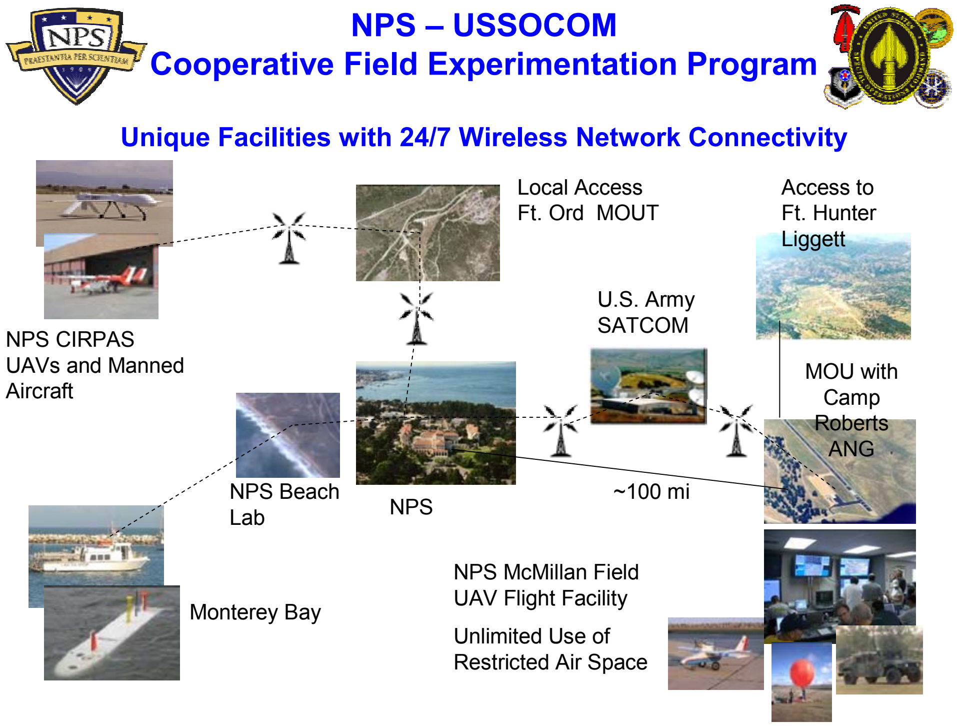


Figure 1. NPS USSOCOM Cooperative Field Experimentation Program

Figure 2. Light Reconnaissance Concept Vehicle TNT 05-2

Beyond the in-house 802.16 OFDM TNT backbone from Monterey to Camp Roberts, the CENETIX test-bed reaches out to numerous and variable assets via Virtual Private Networks (VPN). VPN reach-back to assets like TACSAT in Washington DC, Fort Bragg North Carolina, USSOCOM in Tampa Florida, Biometrics Fusion Center in West Virginia, and Lawrence Livermore National Laboratory allows CENETIX research students to interact and collaborate with nearly unlimited expert services during the scenario driven experimentation (Figure 3). The VPN connectivity not only allows the Naval Postgraduate School and CENETIX to interact with the individual entities, it also allows each of the participants in the network to talk and collaborate with any other participant in the network through the common connection.

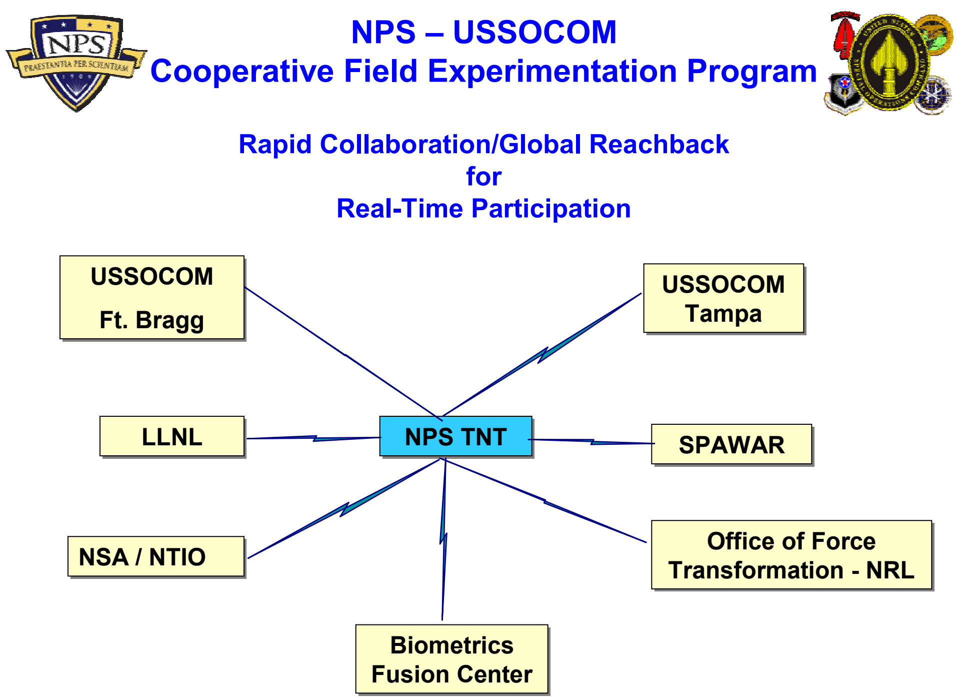


Figure 3. Cooperative Field Experiment VPN Connectivity

The continued expansion of the TNT network will soon include nodes in San Diego California, San Francisco Bay California, and the Swedish National Defense College.

B. PARTNERS IN COLLABORATION

The AN-50M research in CENETIX is supported by all the collective partners mentioned above however there are three stake holders Lawrence Livermore National Laboratory, Innovative Survivability Technologies, and the Biometrics Fusion Center that through development, vision, and operational objective have direct ties to the technology and expert services that support the concept of operations baseline developed later in the thesis.

1. Lawrence Livermore National Laboratory (LLNL)

In addition to providing expert service LLNL is keenly interested in the maritime security dominance domain as part of homeland security. The Lawrence Livermore National Laboratory in conjunction with the Naval Postgraduate School is currently working to extend the TNT network by constructing a maritime security test-bed on San Francisco Bay. The proposed network will extend a radio network data link of 10 Mbps or more from LLNL to the MARAD fleet in Alameda, and Suisun Bay on the north side of Oakland.

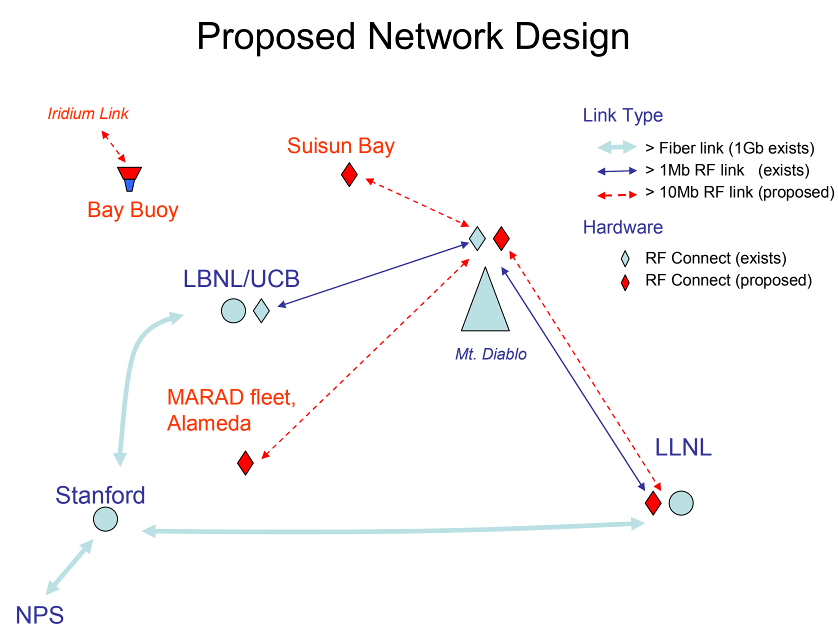


Figure 4. Proposed Maritime Security Domain Network

The proposed extension of the maritime security test-bed into the San Francisco bay area will be the first step to achieving the formidable task of monitoring and protecting port facilities and shipping lanes from criminal and terrorist use.

LLNL is also deeply involved with research and development of Ultra-wide band RF (UWB) data links to be used, among other things, transmitting data from the interior of cargo vessels to portable back-haul devices such as the AN-50M for near real-time situational awareness. UWB radio technology is a promising solution to the difficult RF propagation path variables experienced while transmitting inside ship's hulls and cargo containers. In addition to UWB, LLNL is also assisting in the commercial development of portable self contained radiation source detection and identification equipment to support Navy and Coast Guard VBSS missions.

2. Innovative Survivability Technologies (IST)

Innovative Survivability Technologies focus in the maritime security domain is development of the GN5, a portable Germanium crystal radiation detection and identification device. Larger commercial radiation detection units utilizing sodium iodide detectors and smart identification of know sources have already been developed by IST. These units have been fielded and installed at California's Mexican border crossings and in selected areas of the California Highway system. The in-road systems have been operated with great success, identifying and classifying radioactive sources in vehicles moving at speeds near 60 mph. One of the primary quality attributes of IST's system is ease of operation that allows modestly trained personnel to positively identify radioactive sources even when they are imbedded in materials designed to distract or mask the radioactive signature. The data base and knowledge engine of the system provides rapid classification to operators on the type of source detected with minimal outside analysis required. The fast classification speeds up the scanning process and allows more vehicles to be scanned in a given time period.

In conjunction with LLNL, IST is applying lessons learned from their larger systems to develop a portable Germanium crystal detection and classification unit that is hardened for field use and weighs 15 pounds or less. The difficulties in producing and operating any Germanium crystal detector, including portable units like the GN5, are the physical constraints of the crystal and operating environment. Germanium is preferred

over other super conductors because of its excellent detection resolution. In order to operate however, the crystal must be cooled and maintained at nearly 90 kelvins (-300^{o} F). Typically in large non-portable Germanium units liquid nitrogen is used to cool the crystal. In the case of the GN5 and other portable devices, this is not possible do to size and a limited power supply. The IST solution uses a low power adaptation of a "low noise" commercial phone cell antenna mechanical cooling unit. The mechanical unit cools the germanium crystal and maintains the appropriate operating temperature using only 12 watts of power. After an initial cool down period the GN5 or similar device can operate indefinitely using "hot swappable" batteries. Figure 5 below shows a graphical representation of a portable Germanium crystal radioactive source detector. (Rennie, 2003)

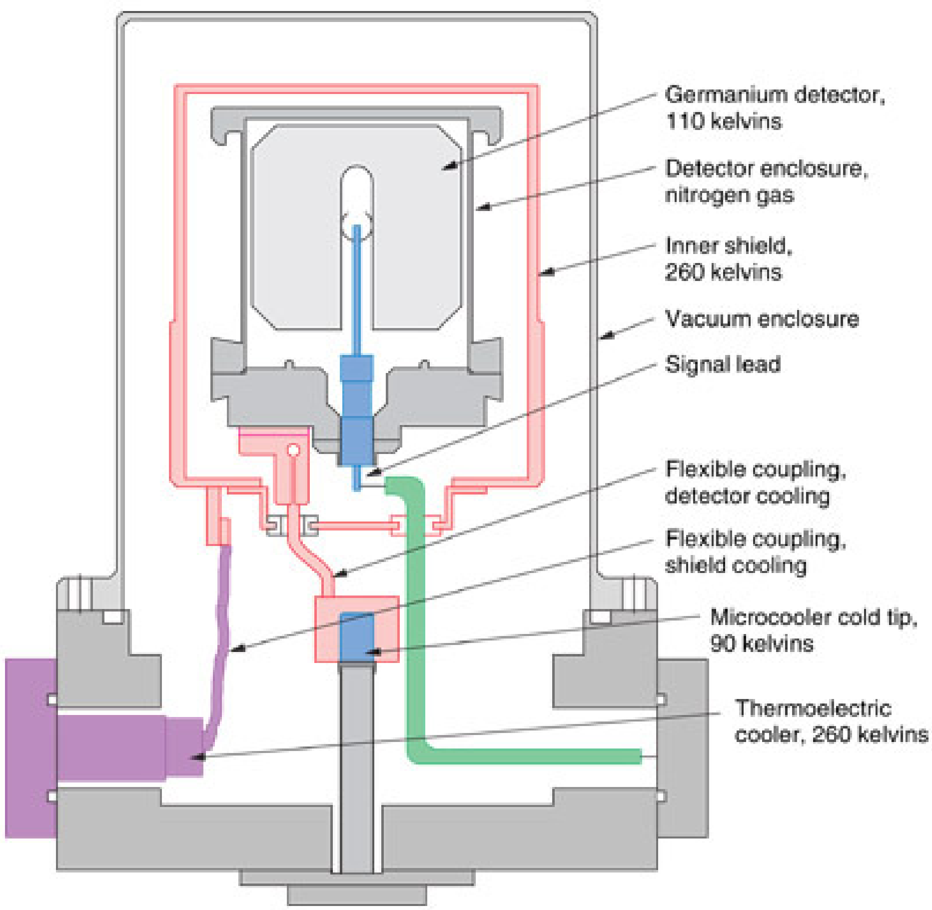


Figure 5. Mechanically Cooled Germanium Crystal Radioactive Source Detector (From: Rennie, 2003)

The IST GN5 production device will not only have the Germanium crystal detector like figure 5, it will also employ a wide angle detection system to provide initial location of radioactive sources, and a method of target source discrimination when the Germanium crystal detector is being used to classify a source. (Adlawan, 2005)

The GN5 and any similar device not only has to meet portability standards, it must be able to survive and operate in the less than desirable conditions of Navy and Coast Guard boardings and port security operations. The GN5 concept unit is specifically being designed and tailored to the ergonomic needs of military and law enforcement personnel and their working environments (Figure 6).

Figure 6. GN5 Concept Device TNT 05-3 IST

3. Biometrics Fusion Center

The National Biometric Fusion Center in West Virginia is an indispensable expert service for frontline forces in the Global War On Terror and state or local law enforcement. In the context of this thesis the dominance of the maritime domain requires the positive identification of threats posed by WMDs such as radio active material and the people who would use or conspire to use these weapons. The National Biometric

Fusion Center collects and stores biometric data gathered from suspects and terror crime scenes world wide. Their data base is designed to be a single point repository of biometric forensic evidence that is accessible to federal, state and local law enforcement and the DoD.

The tight security measures of air travel make shipping lanes one of the most likely methods of smuggling terrorists and terror collaborators around the world. In order to combat the movement of terrorist forces at sea, biometric data like that maintained by the Biometric Fusion Center must be rapidly available to Naval and Coast Guard VBSS teams upon boarding a suspect vessel. Biometric data must be gathered, transmitted, analyzed and returned to boarding teams within the time allotted for a boarding. Typical VBSS boardings may last only a mater of hours, and in some special case even less, thus the rapid turn-around of biometrics data is critical. CENETIX and the Biometric Fusion Center are collaborating to demonstrate that biometric data can be gathered, processed, and leveraged as a sea power asset in a timely manner.

C. THE COLLABORATIVE ENVIRONMENT

The TNT network, and expert services provided by CENETIX partners, combine to form a tactical collaborative environment. The physical link of the environment is provided by the various network components, nodes and protocols such as the wireless 802.16 OFDM, ITT mesh, and ultra-wide band. The virtual collaborative environment is facilitated through the use of software tools. The primary tool for collaboration is Groove Networks “Groove Virtual Office”. Recently purchased by Microsoft, Groove provides any user that is connected by a network (either LAN or Internet) the ability to participate in a common, self synchronizing work space. Data posted by any node in Groove will be automatically shared with all other connected nodes in the same workspace. Nodes that are out of contact will hold outgoing data and self synchronize incoming and outgoing data when connectivity becomes available. On top of file sharing, Groove also provides real-time text chat, voice over IP, and streaming video connectivity.

The second tool used to a great extent in our VBSS experiments is the CENETIX in-house developed situational awareness tool "SA". SA uses a web-based Macromedia Flash Applet to continuously project near real-time data into a two dimensional map of the operating area. Data such as positional icons, alerts and messages associated with various nodes are projected into the map. While Groove is primarily human operator driven, SA takes and post inputs received primarily from automated or machine controlled nodes, but does allow human interface to post amplifying data. Information such as GPS, video, audio, seismic, and some human input are collected and displayed via a central server to the rest of the network.

Groove and SA complement each other well and provide an excellent network centric view of the mission area. Of the two tools Groove is extremely robust and provides excellent survivability characteristics based on its non-nodal pure peer-to-peer connectivity. Provided the network has good self healing or "mesh" properties, the loss of any node in Groove will not effect the sharing of data between the remaining nodes. SA, on the other hand, relies on a nodal configuration in the form of the SA server. While it provides an excellent situational awareness picture, the nodal configuration inevitably offers a single point of failure. For more information on the operation of Groove and SA, refer to the bibliography in the thesis of LCDR Jadon Klopson and LCDR Stephen Burdian USCG titled *Collaborative Applications Used in Wireless Environment at Sea for Use in Coast Guard Law Enforcement Missions,* where these tools and their associated operation are covered in much greater depth. Additional information on Groove can be obtained at www.groove.net.

THIS PAGE INTENTIONALLY LEFT BLANK

III. TESTBED CONFIGURATION

A. 802.16 OFDM OVERVIEW AND THE AN-50E

The IEEE 802.16 standard covers a range of 802.16 sub-standards that use Orthogonal Frequency Division Multiplexing (OFDM) as the wireless physical layer on frequencies ranging from 2-66 GHz. (Eklund, 2002) 802.16 is not the only standard that uses an OFDM wave form. Among others, the IEEE 802.11 a and g Wi-Fi standards also use OFDM. The OFDM wave form uses multiple carrier waves to take the place of and carry the data of one large wave (Figure 7). One of the key benefits of OFDM is that the multiple carrier waves also overlap. This overlap provides very efficient use of the frequency bandwidth by packing more data into the bandwidth with overlapping carriers than can be achieved with a single larger carrier wave spread across the same spectrum. (Redline, 2003)

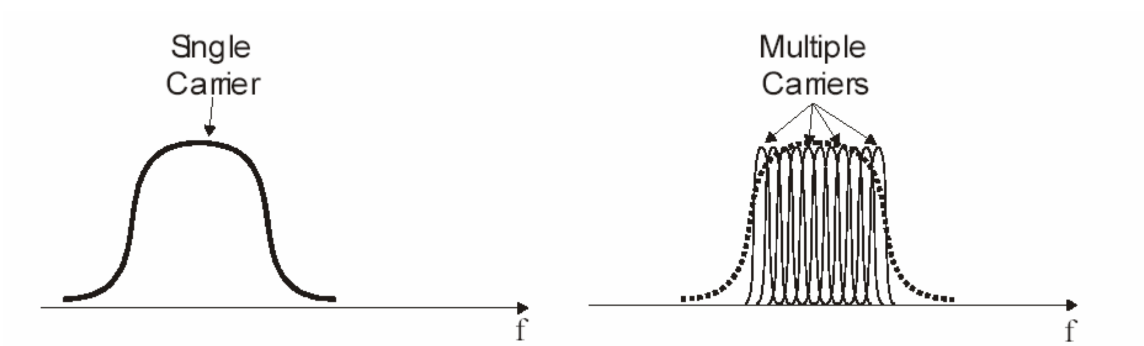


Figure 7. OFDM Wave Form Example (From: Redline, 2003)

While similar in wave form, the major difference between 802.16 and the more well know 802.11 is the way it’s Media Access Control (MAC) admits subscriber stations into the network. 802.11 is primarily used in Wireless Local Area Networks (WLAN). The WLAN, familiar to many of us in small home routers and wireless access points, is designed to cover only hundreds or thousands of square feet. WLANs operate at very low power to prevent frequency interference from many WLANs in a single area. 802.16 on the other hand, is defined as a Wireless Metropolitan Area Network (WMAN) and is designed to cover an area of tens or even hundreds of square miles.

The TNT network uses the Redline Communications AN-50e 802.16 compliant transceiver for both fixed wireless backhaul and mobile broadband networks. Specifically, the AN-50e operates under the 802.16a protocol that identifies devices operating in the 2-6 GHz frequency range. The frequency range for the AN-50e is 5.4 to 5.8 GHz however North American regulations limit the frequency range from 5.735 to 5.815 GHz. The AN-50e radios are designed to operate in a point-to-point or point-to-multipoint configuration depending on the options code purchased with the radio and the firm ware load out. (Redline, 2005)

Covering distances measured in miles rather than feet with a wireless network presents numerous challenges that must be overcome to provide reliable wireless service. These challenges include but are not limited to: interference by other wireless devices, Media Access Control (MAC), spectral efficiency, and in the case of many high frequency microwave links, Fresnel zone interference.

1. RF Interference

One of the primary deficiencies of many proprietary and nonproprietary wireless networks is interference caused by other equipment operating on similar frequencies. Typically wireless networking devices, including those using IEEE 802.11 b and g that operates at 2.4 GHz, use the unlicensed frequency band from 2 – 3 GHz. Other common devices that use this frequency include cordless telephones, microwave ovens and FRS type walkie-talkie radios. (Redline, 2002) Not only is interference from external devices a problem but, because so many devices use the radio spectra near 2.4 GHz strict power output regulations are put in place by the FCC to control the amount of interference between devices. The regulated low output provides additional challenges to long distance use. To combat interference shortfalls the AN-50e operates in an unlicensed frequency range of 5.4 and 5.8 GHz and is above the 2-3 GHz range that most cordless phones, microwave ovens, and other wireless networking devices use. (Redline, 2005)

2. Media Access Control (MAC)

The Media Access Control is the portion of a protocol that dictates how two or more devices communicate on the network. There are numerous methods to accomplish orderly network communication. Some of the better know methods are Carrier Sense Multiple Access with Collision Detection (CSMA/CD) used by Ethernet. Nodes on an

Ethernet network using CSMA/CD essentially listen to the common carrier to see if another node is communicating. If the line is open then the node is free to send traffic. If there is communication already in progress then the rest of the nodes wait to send data. If two nodes begin sending at the same time, a collision is detected and both nodes subsequently back-off and wait a random time period, measured in milliseconds, before attempting to send again. (HSW-1, 2005)

The 802.11 protocol uses a similar method to Ethernet called Carrier Sense Multiple Access Collision Avoidance (CSMA/CA). CSMA/CA works well when a large majority of the clients in a given network are able to hear each other. Much like a room full of polite people the various nodes sense when someone else is talking and refrain from transmitting until the network is clear. The CSMA/CA Media Access Control however, begins to break down and become inefficient when employed in large WMANs. The break is due to the large distances in WMANs between nodes, causing the nodes to be unaware of the other nodes on the network. In this scenario, network traffic is sent in the blind using random chance to avoid a collision with another transmission. The blind transmission causes collisions to increase, thus prompting data to be resent. As the number of nodes that cannot hear each other in the network increase, the CSMA/CA MAC becomes more and more inefficient as more and more collisions require retransmission of data. (HSW-2, 2005)

The 802.16 Media Access Control is much more adept to deal with the challenges of a WLAN. Rather than relying on a system where other nodes must be able to hear each other in the transmission medium such as CSMA/CD or CSMA/CA, the 802.16 MAC uses Time Division Multiple Access (TDMA). TDMA assigns time slots to individual nodes for data transmission. Provided any given node can hear the base station for synchronization there will be no conflict with data transfer using TDMA. Although there is somewhat more management overhead that must be broadcast and time synchronization is much more critical, TDMA provides an excellent solution to WMANs that have nodes distributed over larger distances. (Redline, 2003)

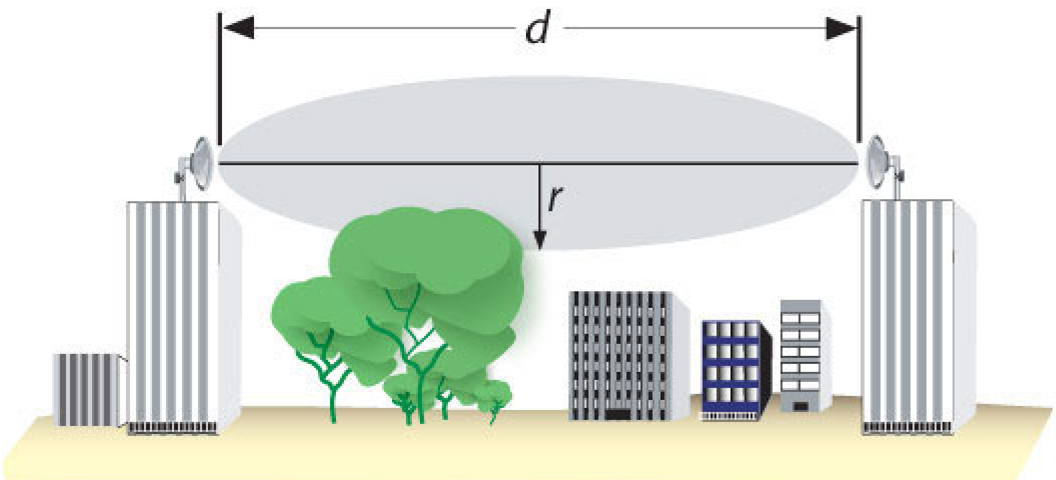
3. Spectral Efficiency

Adding to the spectral efficiency of the 802.16 protocol achieved by OFDM is the Redline AN-50e's use of adaptive modulation. The AN-50e is capable of using BPSK,

QPSK, QAM 16, and QAM 64 data compression. Because conditions over the data link can change rapidly, the AN-50e dynamically shifts between the data compression schemes to maintain the lowest bit error rate and provide the highest throughput that the link will support. The AN-50e also employs Time Division Duplexing (TDD) to make further use of the radio spectrum available. TDD allows the AN-50e to communicate both upstream and downstream in the same frequency band, thus making more efficient use of the available bandwidth. (Redline, 2002)

4. Fresnel Zone Interference

Fresnel zone interference is particularly problematic with microwave links. The High frequency microwaves are also particularly susceptible to absorption by water molecules. The same concept is applied to heat foods and liquids in a microwave oven. The Fresnel zone is the area that a wave spreads into after it leaves an antenna. Depending on the length of the link even a line-of-sight link, can have substantial interference by objects that protrude into the radius of this zone by more than 20 percent. Figure 8 provides a graphical representation of the Fresnel zone profile and associated mathematical calculations. (TBW, 2005)



$$r_{(\text{in mts})} = 17.32 \times \sqrt{\frac{d_{(\text{in Km})}}{4f_{(\text{in GHz})}}} \qquad r_{(\text{in ft})} = 72.05 \times \sqrt{\frac{d_{(\text{in miles})}}{4f_{(\text{in GHz})}}}$$

Figure 8. Calculation of the Fresnel Zone profile (From: TBW, 2005)

B. TNT 802.16 OFDM BACKBONE

The student developed and operated TNT network uses 802.16 compliant AN-50e broadband WMAN transceivers produced by Redline Communications. Currently all the AN-50e radios operated in the TNT are configured to operate on a point-to-point basis. The TNT backbone extending from the Naval Postgraduate School to Camp Roberts near Paso Robles California consists of twelve AN-50e radios that use 5 intermediate relay stations to complete a 120 mile link. The distance between relay stations ranges from 100 yards to a 39 mile link between Bryant and Williams hills passing over King City California. Due to the large link distances, multi-path and RF interference, the backbone uses a maximum of QAM 16 data compression for 18 Mbps through-put. Once communications are established between nodes, configuration and monitoring of each node are made easy through SNMP agents and a simple to use web-enabled GUI interface show (Figure 9).

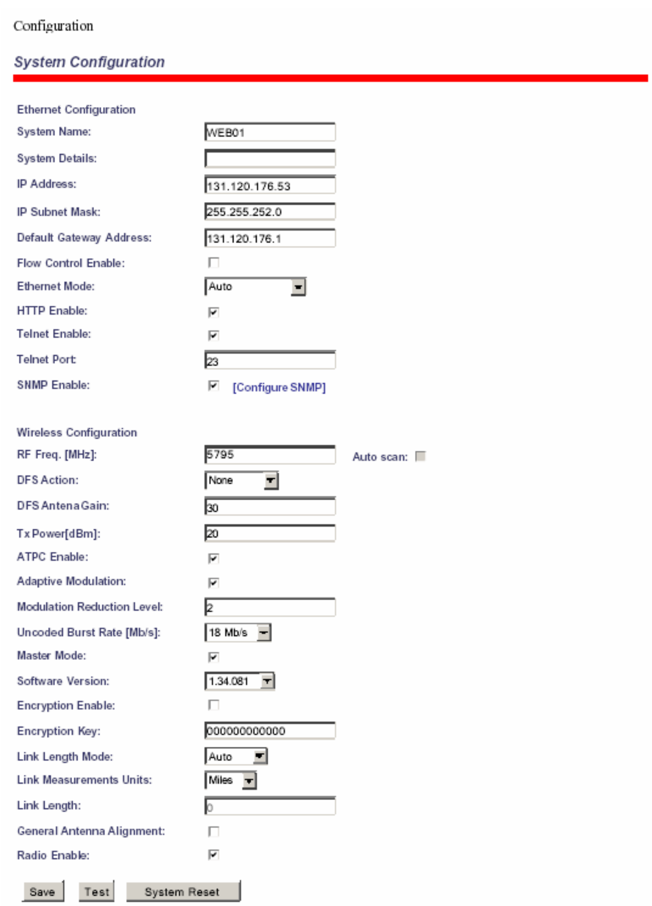


Figure 9. Redline AN-50e web-enabled configuration GUI

Backbone health and connectivity are monitored at either the Camp Roberts Tactical Operations Center (TOC) or the Naval Postgraduate School Network Operations Center (NOC). Software monitoring of all nodes attached to the backbone is accomplished primarily through the Solar Winds network monitoring suite using SNMP agents.

C. OFDM EXTENSION TO SEA

1. Software Controlled Variable Sector Point-to-Point Link Antenna Configuration

Located ½ mile northwest of the Naval Postgraduate School, the Del Monte Beach Lab is the point where the TNT network is project to sea. The Del Monte Beach Lab's AN-50e radios provide 802.16 coverage of the Monterey Bay out to a range of six miles. In order to facilitate the best link budget to the coverage area, three 60 degree sector antennas are used at the Beach Lab. The Three antennas are configured through software to be a point-to-point link. Sensing which antenna has the highest signal strength, the antenna configuration software selects that radio and antenna for transmission while keeping the other two radios silent. The two remaining radios and antennas stay offline until such time that the target node moves into the sector of one of the other radios and the software shifts the active sector. The graphic (Figure 10) shows the coverage area of sector two as it appears in SA when it is active.

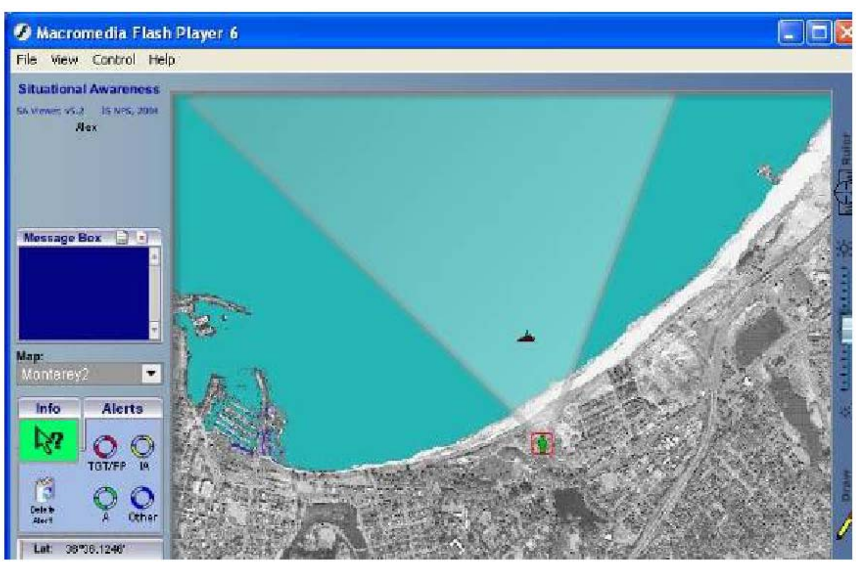


Figure 10. View of Beach Lab sector 2

2. The Del Monte Beach Lab

The Del Monte Beach Lab, represented in figure 10 by the small green "man" figure, is the focal node for the 802.16 OFDM coverage of Monterey Bay. From the Beach Lab wireless 802.16 point-to-point traffic is relayed by one of two methods to the Naval Postgraduate School NOC. The first method is via another 802.16 OFDM link to the top of Spanagel Hall and from there by a short wireless link to Root Hall where the NOC is located. The second more recent method is back-haul via the Naval Postgraduate School's LAN on the 131.120.x.x network using a fiber optic link back to the Naval Postgraduate School. Once on the campus, 131.120.x.x network IP traffic is routed via a logical bridge that connects the TNT 192.168.x.x network.

3. Link Budget

The theoretical link budget and Freespace path loss figures for a point-to-point link between the Del Monte Beach Lab and the Cypress Sea research vessel are calculated using the following Freespace path loss equation. (Kathein, 2005)

Freespace Path Loss

$$L = 96.6 + 20 \log(d) + 20 \log(f)$$

Where:
L = freespace path loss
d = distance in miles
f = frequency in GHz

The distance variable of the equation is dynamic due to Cypress Sea's mobility on the bay. The antennas used in the link are 60 degree sectors at the Beach Lab and a 16 inch omni-directional antenna on the mast of Cypress Sea. The 60 degree sector antenna has a manufacturer rated signal gain of 16 dBi. The omni-directional antenna on Cypress Sea has a manufacturer rated signal gain of 9 dBi. Documentation provided by Redline Communications indicates that the receiver sensitivity of the AN-50e is -86 dbm. In practical application on the TNT network it has been noted that any link below -79 to -80 dbm is generally unstable, especially when combined with a sea node that is subject to wave action. The combined transmission gain added to the antenna gain in decibels must be enough to achieve a link that is -80 dbm or better to maintain stability. The generic formula for this is as follows: (20 dBm transmission) + (16 dBi sector antenna gain) + (9 dBi omni gain) – (Freespace path loss in dBm). Table 1 depicts link budget figures for the Beach Lab to Cypress Sea link out to seven miles in ¼ mile increments.

Distance in Miles	Freespace Loss in decibels	Calculated Received Signal Strength in decibels
0.25	99.83	-54.83
0.50	105.85	-60.85
0.75	109.37	-64.37
1.00	111.87	-66.87
1.25	113.81	-68.81
1.50	115.39	-70.39
1.75	116.73	-71.73
2.00	117.89	-72.89
2.25	118.91	-73.91
2.50	119.83	-74.83
2.75	120.66	-75.66
3.00	121.41	-76.41
3.25	122.11	-77.11
3.50	122.75	-77.75
3.75	123.35	-78.35
4.00	123.91	-78.91
4.25	124.44	-79.44
4.50	124.93	-79.93
4.75	125.40	-80.40
5.00	125.85	-80.85
5.25	126.27	-81.27
5.50	126.68	-81.68
5.75	127.06	-82.06
6.00	127.43	-82.43
6.25	127.79	-82.79
6.50	128.13	-83.13
6.75	128.45	-83.45
7.00	128.77	-83.77

Table 1. Freespace loss and associated received signal strength for a link using a 60 degree 16 dBi sector to 9 dBi omni antenna at 5.8 GHz and transmission gain of 20 dbm

Table 1 link connectivity and stability should be theoretically reliable out to a range of 5 to 5.25 miles using a conservative receiver sensitivity figure of -79 to -80 dbm. Using the Redline Communications receiver sensitivity figure of -86 dbm, theoretically the link would be stable beyond 7 miles. All of the calculations above discount environmental attributes such as wave action, atmospheric conditions and on-shore foliage penetration that will all combine to reduce the link stability and range of the link.

4. Tracking Antenna Concept

The current configuration of the Del Monte Beach Lab, as mentioned above, is constructed to provide point-to-point coverage of the entire Monterey area of Monterey

Bay. Coverage is provided out to a range of 6 miles to a single target using 3 AN-50s identically configured and controlled by software. This method, while functional, is wasteful in equipment usage for a single point-to-point link. A better method that is to be employed in future TNT experimentation is the use of a "smart" tracking antenna. The "smart" antenna uses GPS to track the Cypress Sea research vessel and direct a single antenna rather than the current array. The use of a "smart" antenna not only reduces AN-50 use by two thirds at the Beach Lab, it also provides better link budget by using a narrow beam directional antenna opposed to the 60 degree wide beam sector antennas that are currently employed.

The prototype GPS tracking antenna uses 900 MHz out of band signaling through Freewave Communications radios to transmit GPS data to the tracking antenna. The 900 MHz radios have longer range than the 5.8 GHz link, so initial antenna alignment will be accomplished before the 5.8 GHz link is within range to be established. In the future GPS data could potentially be sent over the 802.16 OFDM data link once initial antenna alignment is achieved and a stable link established. The best solution however, may be to use both the 900 MHz and 802.16 link as a form of multi-band redundancy for antenna alignment.

D. BOARDING PARTY LOCAL AREA NETWORK

Once onboard a suspect vessel, boarding teams require connectivity for various activities such as biometric data gathering, radiation detection, text messages, voice, video, and other collaborative efforts. The boarding party LAN used in TNT experimentation is a two-part network. The first part of the network is a standard 802.3 Ethernet. The 802.3 network is established by connecting the AN-50M Man-Pak to a standard 5 port 100 Mbps Ethernet switch using a standard RJ-45 cross-over cable. The 5 port switch is powered by a Mil-5590 (non-rechargeable) or Mil-390 (rechargeable) 12/24 volt battery configured with both battery cells in parallel to provide 12 volts dc power. Fanning out from the 4 remaining ports on switch is connectivity for biometrics data acquisition, boarding officer command and control, and connectivity for the LLNL Ultra Wideband network.

The LLNL Ultra Wideband (UWB) is the second part of the boarding party network. Ultra Wideband radio network technology uses a broad frequency spectrum to provide better multi-path connectivity rather than high data transfer rate. The UWB network is employed to penetrate multiple decks on the boarded ship through steel bulkheads and other impedances that typical narrow band and higher radio networks fail to negotiate.

During experimentation with The Naval Postgraduate School, LLNL UWB links have been established with LLNL laptop computers that house the proprietary software used in UWB communications. LLNL laptops are linked to the TNT network by the aforementioned 802.3 Ethernet boarding party LAN and backhauled by an 802.16 Redline OFDM network (Figure 11).

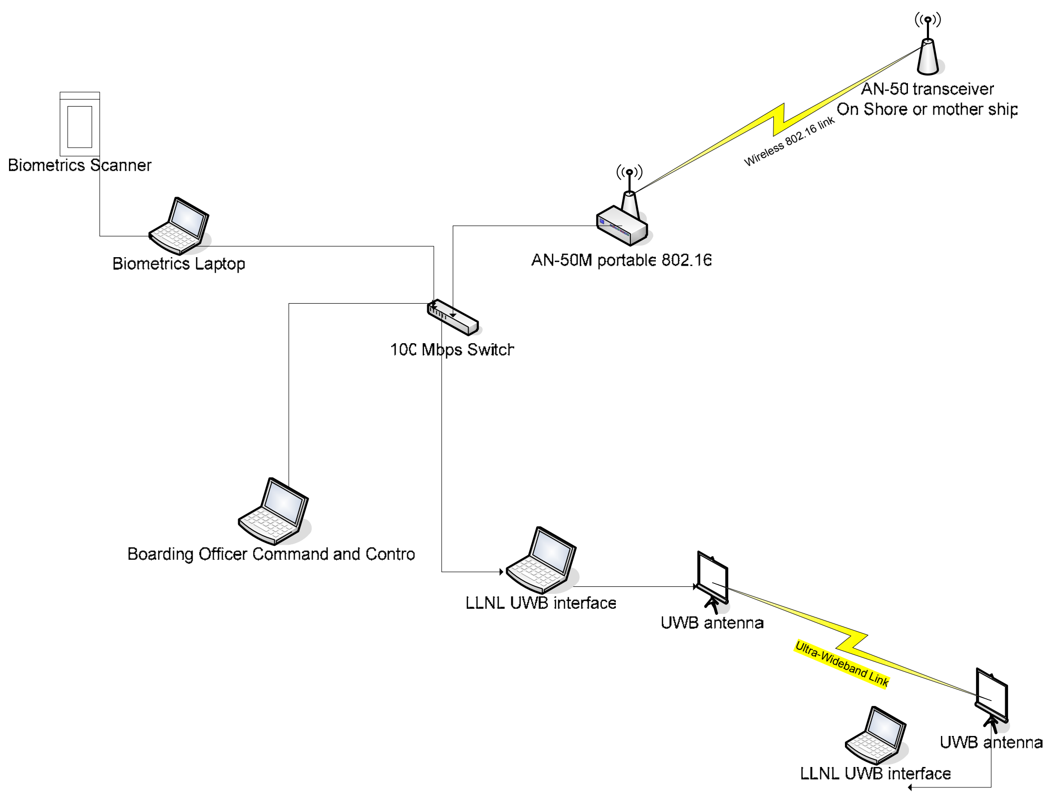


Figure 11. Boarding Party LAN diagram

IV AN-50M MAN PORTABLE 802.16 OFDM PROTOTYPE FUNCTIONALITY AND FUTURE REQUIREMENTS

A. THE AN-50M

Aside from appearance the AN-50M functionally is virtually identical to the standard Redline Communications AN-50e 802.16 wireless radio. The exterior of the AN-50M is a hardened ruggedized case that has been coated in a dull olive drab to reduce visibility for military applications. The cooling fans have been removed from the case to provide a measure of weather resistance. Over heating is not a problem as the electrical components of the AN-50 do not generate large quantities of heat. The fact that the rack mounted version of the AN-50 has chassis cooling fans is more a function of redundancy than necessity. Along with a ruggedized case, shoulder straps have been added for carry and portability. Brackets have been installed on the opposite side from the shoulder straps to hold 2 Mil-5590 or Mil-390 batteries, a 16 inch 9 dBi omni-directional antenna and the T-58 transceiver (Figure 12).

Figure 12. AN-50M Portable 802.16 OFDM Prototype

B. ANTENNA CONFIGURATION AND CONNECTIVITY

AN-50M connectivity is generally established using the attached 9 dBi omni-directional antenna to another AN-50 device using one of many types of antennas. Although the primary antenna for the AN-50M is the installed omni directional, like any AN-50 it can use the full array of sector or directional antennas. The installed omni directional antenna is adequate but it is a structural weak point and source of unwieldy ergonomics due to its single piece rigid construction and non-flexible mounting. The AN-50M would be much better served by an antenna system similar to that used on the military Enhanced Position Reporting and Location Radio System (EPLRS). The installed EPLRS antenna uses a flexible base and allows the antenna to be directed skyward regardless of the inclination of the radio and does not present a weak point that shears off at the first obstacle it encounters.

Typically when employed in a ship boarding scenario the AN-50M will be communicating to a 60 degree 16 dBi sector antenna or possibly a smart tracking antenna on a base station while using the installed 9 dBi omni locally. When communicating to a 60 degree 16 dBi sector antenna through its 9 dBi omni, the link budget figures provided in table 1 will be applicable. In certain situations, such as the use of multiple AN-50Ms to a multipoint base station, an omni direction to omni direction connection may be desirable. The use of an omni directional antenna on both ends of the link will reduce the effective range and throughput of the link, but will allow 360 degree coverage from the base station. Table 2 shows the theoretical Freespace path loss for a 9 dBi omni-to-omni connection. The omni-to-omni link remains above the conservative -80 dbm threshold out to a range of 2 miles. Using manufactures specifications of -86 dBm, a link should be stable through 4 miles. One must keep in mind however, that the data below assumes optimal antenna placement with no Fresnel zone or other interference. Since optimal antenna placement is rarely achieved in field operations it is a safe assumption that the ranges in Table 2 will be less effective on a case by case basis.

Distance in Miles	Freespace Loss in decibels	Calculated Received Signal Strength in decibels
0.10	91.87	-53.87
0.20	97.89	-59.89
0.30	101.41	-63.41
0.40	103.91	-65.91
0.50	105.85	-67.85
0.60	107.43	-69.43
0.70	108.77	-70.77
0.80	109.93	-71.93
0.90	110.95	-72.95
1.00	111.87	-73.87
1.10	112.70	-74.70
1.20	113.45	-75.45
1.30	114.15	-76.15
1.40	114.79	-76.79
1.50	115.39	-77.39
1.60	115.95	-77.95
1.70	116.48	-78.48
1.80	116.97	-78.97
1.90	117.44	-79.44
2.00	117.89	-79.89
2.10	118.31	-80.31
2.20	118.72	-80.72
2.30	119.10	-81.10
2.40	119.47	-81.47
2.50	119.83	-81.83
2.60	120.17	-82.17
2.70	120.50	-82.50
2.80	120.81	-82.81
2.90	121.12	-83.12
3.00	121.41	-83.41
3.10	121.70	-83.70
3.20	121.97	-83.97
3.30	122.24	-84.24
3.40	122.50	-84.50
3.50	122.75	-84.75
3.60	122.99	-84.99
3.70	123.23	-85.23
3.80	123.46	-85.46
3.90	123.69	-85.69
4.00	123.91	-85.91

Table 2. 9 dBi omni-to-omni Freespace path loss and receive signal strength to 4 miles

C. PORTABILITY

The AN-50M's total weight is just under five pounds. Although it is light, the current form factor leaves room for improvement. The AN-50M has shoulder straps for

backpack style carry however, the width of the straps and the flat case housing do not permit easy or comfortable carry for extended periods of time. The RJ-45 and antenna attachment points are subject to breakage due to protrusion. Future versions of the AN-50M could correct portability issues by mounting to a better backpack style frame like that used by U.S. Military ALICE packs. Moving the antenna and RJ-45 connection points to the sides rather than top and bottom would reduce breakage by inadvertently sitting the full weight of the unit on one of the stress points.

D. POWER REQUIREMENTS

The AN-50M is configured to run on 1.5 Amps of 12 volts dc current. The required power is easily provided by two Mil-5590/390 12/24 volt batteries. In field testing, during TNT 05-4 and in the CENETIX lab, the AN-50M exhibited excellent power consumption rates. On fully charged batteries, typical continuous transmission time is between 8 and 10 hours. Power consumption by the 100 Mbps switch is negligible with no appreciable power drain in over 20 hours of operation on the same Mil-390 battery. In all AN-50M experimentation the limiting power factor has been battery life on the laptop computers and other peripheral equipment.

E. ADDITIONAL HARDWARE AND SOFTWARE

The AN-50M requires no additional software or hardware to transmit IP traffic once it is configured. To configure the AN-50M however, use of a laptop computer via a GUI web browser interface is required. Configuration is accomplished by entering the AN-50M's IP address in the address line of an open web browser window. In order to connect with the AN-50M the computer's network interface card (NIC) must be in the same network IP space as the AN-50M. For example, if the AN-50M's IP address is 192.168.25.2 (factory default) the computer used to configure the AN-50M must have its NIC IP address set to 192.168.25.X where (X) equals any number 1-254 except for 2 in this case. The AN-50M can also be configured using a VT100 terminal connection and command line interface. (Redline, 2004)

Beyond device configuration, monitoring of the wireless link status is accomplished using a laptop that has Redline Communication's RFmonitor software installed. The RFmonitor software is a small and easy to use program. To monitor a link using RFmonitor, connect to the AN-50M by entering its IP address into the setup window and selecting "connect" followed by "done" Once connected, RF monitor provides a graphical representation of the wireless link by showing receive signal strength and signal-to-noise ratio. After a link is established and stable, the remote AN-50 receiver can be monitored in conjunction with the local link. In RFmonitor setup the connection to the local link is achieved as above. After connecting to the local link, and before selecting "done" move to the remote side of the setup dialog box and connect to the remote AN-50. After connecting to the remote system choose "done". The graphical representation will now show two simultaneous performance lines in both receive signal strength and signal-to-noise ratio. The red line represents the local system and the blue line represents the remote system in both graph windows.

To alleviate the need for a separate laptop to make configuration changes in future AN-50M models, the use of an incorporated processor and PDA size touch screen would be an improvement. Incorporation of a modest PC or PDA processor and operating system combined with a small touch-style display would make the AN-50 a "smart" node that could be taken to the field as a standalone device. A further recommendation for the AN-50M is installation of a fixed 5 port 100 Mbps switch. A fixed switch would take the place of the current external switch that must be carried along with a separate power supply. An installed switch could be supplied by the AN-50M power supply, reducing the need to carry separate batteries and wiring harnesses.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCEPT OF OPERATION FOR PORTABLE BROADBAND BACKHAUL

A. CURRENT SHIP BOARDING METHODOLOGY

As stated in the introduction, my personal experience in Visit Board Search and Seizure operations led me to pursue the use of portable broadband backhaul as a tactical tool and force multiplier during ship boarding operations. The conduct of VBSS operations is governed by numerous naval instruction and training documents. Much emphasis has been placed on the safe and secure boarding of a ship, weapons, qualification, and search techniques. The communications methods employed in VBSS operations has been and still is inefficient.

The primary mode of communication between the boarding team and the mother ship is analog voice communication. The voice communication is facilitated by standard two-way walkie-talkie radios. When a suspect vessel is boarded, specific information in the form of a boarding action report must be gathered. The exact contents of a boarding report may vary depending on the type of boarding and individual situation. The specific data types are not important to this operational methodology. What is pertinent is the amount of data gathered and the methods used for capturing, recording, transmitting and archiving the required data.

From my boarding experience in the Arabian Gulf and off the west coast of Mexico, most data was captured by filling out, by hand, a boarding report worksheet on the boarded vessel. After each page of the multiple page worksheet was completed, it was handed to a radio talker who relayed the information to the mother ship where it was again hand scribed into an identical boarding report work sheet. Completed pages of the identical mother ship worksheet were the relayed by DoD SATCOM to the Maritime Interdiction Operation Warfare Commander. After the voice relay all the information was transcribed into naval message format and sent upon completion to numerous recipients.

The voice communications relay of information gathered during a VBSS boardings requires in most cases a minimum of 3 scribes and 3 radio talkers to process

and route data to the required destinations. The radio communication requirements in a VBSS operation are manpower intensive and wasteful. In some cases a radio alone cannot capture all the required data. Data such as photographs, documentation, video and audio recordings, etc. must be collected onsite, bagged in water proof packaging and transported by small boat back to the mother vessel. Once onboard the mother ship, physical documents must be photocopied and the originals returned to the suspect vessel by small boat. A round trip from suspect vessel to mother ship and back requires three personnel in the small boat and the time required to transit between the vessels and wait for copies of the material to be completed.

B. TRANSITIONING TO THE DIGITAL MEDIUM

The time required to transcribe voice communications into multiple data streams and transport photos, video, and documentation via small boat for reproduction and physical shipping is extremely manpower intensive. Aside from time and manpower the requirements of the GWOT have drastically changed the amount, type, destinations, and speed requirements for VBSS data handling. To maximize team effectiveness, reduce redundancy or data transcription and speed up transfer, a shift to a total digital medium is required.

The transition to digital media has been on going and is now the preferred method for nearly all types of data storage and capture. Digital cameras are rapidly replacing film. Digital video and voice recording have been the industry standard for over 10 years. Portable document scanners and laptop electronic document handling technology is a mature and reliable technology. Digital technology is and has been employed in VBSS operations to varying degrees, however the digital medium is still reliant on traditional methods of backhaul. Although the digital media is more convenient, it is no more efficient than previous methodology because of the reliance on analog, and hand delivery backhaul. The traditional voice and small boat backhaul methodology is stifling the potential leverage of the digital technology being employed.

C. BROADBAND COMMUNICATIONS BACKHAUL

Central to the concept of a digital transformation is usage of a common digital backhaul method with enough bandwidth to handle all the data transfer required by a boarding party. This thesis is focused on use of the 802.16 wireless protocol to provide just such backhaul capability. This concept of operations is not limited to a single protocol. It is however rooted in the premise that sufficient bandwidth for a single mode of digital backhaul is required to take advantage of net centric assets. Using a broadband backhaul carrier eliminates the need for multiple data transformations such as text to voice and back to text. Utilization of broadband networked communication between a mother ship and boarding party facilitates voice, video, and data transfer via a single communications channel that provides two-way communications that are not limited by locality but by network connectivity.

1. Voice Communication

Voice Over IP (VOIP) within a collaborative application like Groove Networks' Groove Virtual Office allows any boarding party team member with connectivity to communicate with everyone in the collaborative workspace (party-line) or selectively and securely communicate with individuals, such as the boarding officer communicating directly with his or her commanding officer.

2. Video Transfer

Real time video transfer from boarded vessels adds to situational awareness. Video can be streamed to all or some of the collaborative participants as bandwidth allows. Digital video can be used to identify high value targets or recorded for future analysis.

3. Digital Data Transfer

Broadband digital communication allows a functional shift in the method that textual and document data are captured and processed. A networked connection such as that provided by the AN-50M would allow remote users to enter boarding report worksheet data directly into an electronic environment such as a web enabled database. Hardcopy documents can be scanned into digital media by using portable document scanners or simply high quality digital photographs. All digital data can be time, date and description meta tag stamped for rapid search and future analysis.

D. EXPERT SERVICE REACH-BACK AND COLLABORATION

Data acquired and transferred in digital form on a common networked communications medium reduces personnel overhead and allows collaboration from multiple points simultaneously in a common operating environment. The networked common operating picture is a force multiplier and the key to the leverage of utilizing broadband digital communications for VBSS operations. Once in the standard TCP/IP communications channel and incorporated into a near-real-time collaborative tool such as Groove, expert service assistance can be used to increase situational awareness and reduce critical decision time. The networked boarding team has the ability to rapidly change and augment it's virtual component to meet dynamic requirements.

As stated in the beginning of this chapter, the rules of engagement concerning data capture and processing in VBSS operations have changed. Traditionally boarding teams could handle basic identification of well defined illicit cargo and known criminals with minimal outside support. More recently potentially hazardous cargo such as radioactive and chemical or biological weapons are less well defined and many times well hidden in what appears to be harmless shipping containers. These weapons, that were once only available to technically advanced nations, are becoming more commonly available and are being assembled, purchased or stolen to augment radical stateless terror organizations. Beyond illicit cargo the shipping lanes of the world are increasingly becoming the prime mover for the personnel of various terrorist networks. As air travel regulations and screening become tighter and more efficient, the relative easy passage of goods and people through merchant port facilities is rapidly becoming a prime focus for The United States and Allied nation's homeland defense. To increases the confidence of stopping an attack through merchant sea trafficking, hundreds, if not thousands, of ships must be boarded and inspect daily by forces world wide. The type, amount, and speed of the required data acquisition and analysis to support combating terrorist use of the shipping lanes is beyond the ability of an unsupported stand alone boarding party.

Total electronic capture, backhaul, and storage is the only method available that properly leverages the network centric warfare model with respect to port and sea lane security. Digital data on the network can be viewed and `analyzed by subject matter experts hundreds or even thousands of miles away. Biometrics data can be processed in

minutes rather that hours or days. The payoff of networked VBSS operations comes in the form of single acquisition seizure or apprehension. In other words, the task of re-aquiring a criminal days or weeks after initial biometrics are taken is difficult and has a low probability of success. The ability to quickly process and know if any suspected criminals are aboard a vessel, based on biometrics, will allow law enforcement and military teams to apprehend on first contact, minimizing the chances of possible escape. This type of specialized service has also been successfully employed during the course of multiple scenario-driven TNT measurements and field trials. In addition to interpretation of radioactive source fingerprints by remote experts can reduce search time and delays while inspecting cargo. In the case of both biometrics and radiation detection analysis collaborative expert services have been shown to be viable in rapidly enhancing situational awareness and are worth further pursuit and implementation. These are only two examples of the reach-back provided to a networked boarding party. The concept of expert reach-back can be applied to limitless possibilities. Near-real-time collaboration by VBSS teams with expert services is crucial to effectively combating the traffic of WMDs and the inviduals who would use them.

E. MISSIONS OTHER THAN MILITARY OR LAW ENFORCEMENT (KATRINA DISASTER RELIEF)

Beyond pure law enforcement and military applications, the ability to rapidly extend a high bandwidth collaborative environment is essential to the timely response of, among other things, civil or natural disasters.

1. Network Configuration

Network configuration varies widely depending on range, line-of-sight (LOS) vs. non-line-of-sight, and throughput requirements. Planning for the wide range of contingencies that may arise in combat, law enforcement, and disaster relief operations is the primary focus for development and planning of rapidly deployable collaborative networks. Breaching the sea-land barrier to provide rapid situational awareness, and connectivity between shore and afloat command and control facilities is crucial to mission success. The following network conceptual deployment plans were developed at the request of United States Navy Second Fleet in response to the need for network

collaboration to aid disaster relief following Hurricane Katrina's landfall and subsequent massive destruction on the Mississippi and Louisiana gulf coast.

a. Link to Vessel Pier-Side

The near-shore anchorage or pier-side links are two of the simplest links to establish. The link between a pier-side ship and the Shore Operations Center (SOC) is the simplest task. Because both ends of the link in a pier-side ship to shore link are relatively stationary, the antenna configuration plan can use a wide variety of the available antennas to provide different networks architectures.

Use of high-gain, narrow beam, directional antennas, to maximize link throughput and protect against jamming, can easily provide throughput at DSL levels through 10 miles if line-of-sight can be established to a tower or tall building. Non-line-of-sight links can be established using reflections off buildings. Using non-line-of-sight techniques, throughput will vary on a case by case basis.

The use of an omni-directional antenna on the ship and an AN-50 configured as a point to multi-point base-station will allow multiple subscriber stations access. Flat panel directional antennas aligned to the omni base-station will provide DSL connection speed out to a range of 2-4 miles depending on terrain and RF interference. Dense urban terrain may limit some ranges to significantly less than that of line-of-sight optimal links. In all tests however, 802.16 links out perform 802.11 wireless links in similar operating environments. Figure 13 depicts graphically both examples of pier-to-shore connection. At the termination of the 802.16 nodes ashore, it is a simple matter to set up standard 803.3 Ethernet LAN, 802.11 Wireless LAN or ITT mesh to facilitate multiple individuals and computers access to the network.

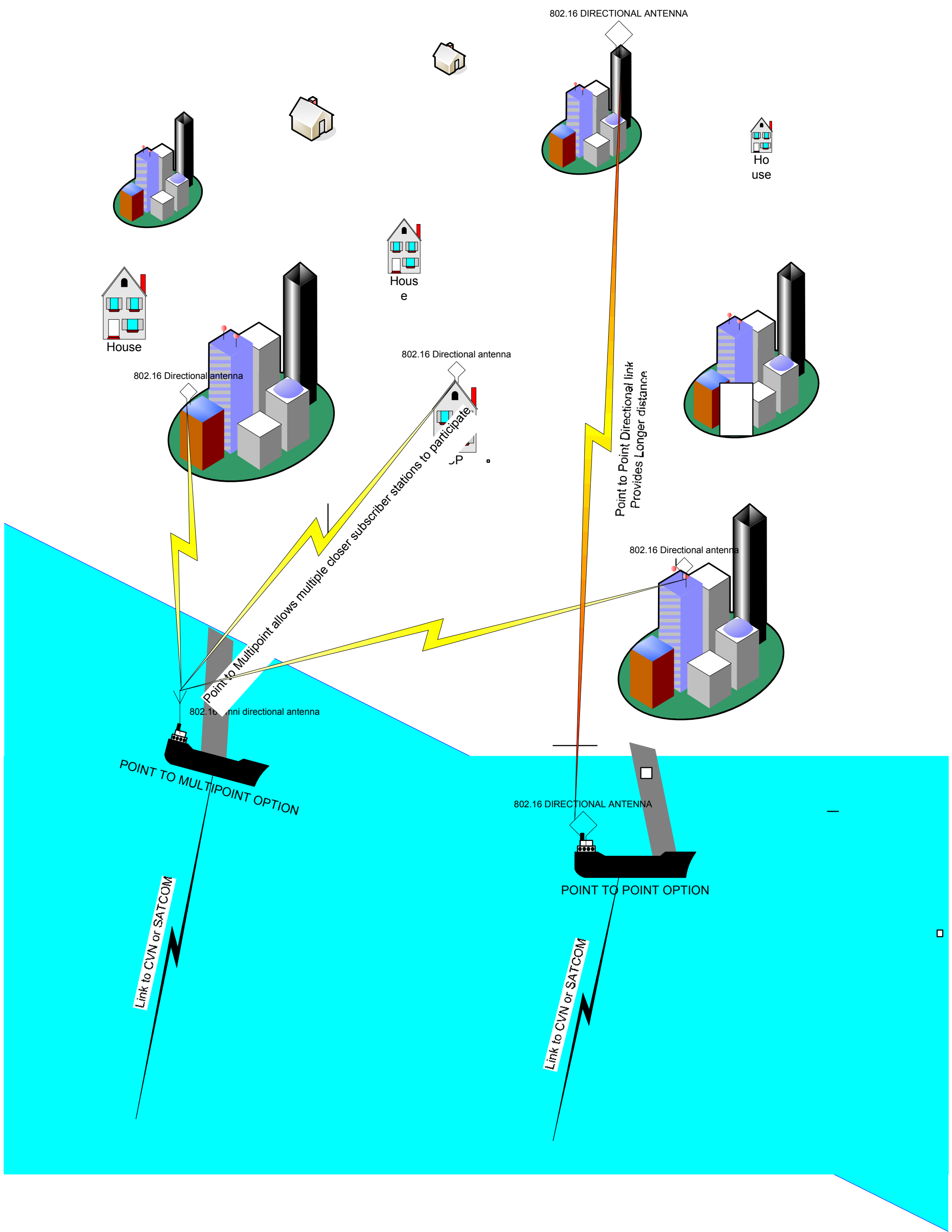


Figure 13. Point-to-point and Point to Multipoint configuration

b. Link to Vessel in Near-Shore Anchorage

Link to a vessel in near-shore anchorage is nearly as simple as a vessel pier-side. The near shore anchorage however, virtually rules out use of a directional antenna on the anchored ship unless a tracking antenna is available. The movement of the ship around its anchor as tidal current flows in out would require constant tracking of

the directional antenna toward the Shore Operations Center (SOC). To alleviate the tracking problem, the near shore anchorage method would use a similar approach to the point-to-multipoint method. An omni-directional antenna would be placed on the anchored ship. The base station or stations would use sector antennas (60 or 90 degrees of arc) to project a cone of connectivity that would cover the width of the ship's swing circle. Recall that figure 10 in chapter 3 depicts what a 60 degree sector cone looks like projected on Monterey Bay from The Naval Postgraduate School's SOC at the Del Monte Beach Lab.

Links using a 60 degree sector antenna to a mobile and stationary ship in Monterey Bay have been successfully tested numerous times. Transmission speeds of 800-900 Kbps were normal at a range of six miles in calm seas as seen in the TNT 05-1 experiment. The inland range and connectivity speed of a shore to near-shore anchored ship is less than can be established by a pier-side ship link because of antenna link budget and the distance of the ship off shore.

c. Backbone Backhaul to Commercial ISP Source.

In order to provide better connectivity and relieve the bandwidth usage from the DoD SATCOM assets, a backbone style backhaul relay chain can be constructed to the nearest commercial ISP that is still connected in or near the disaster area. Currently the Naval Postgraduate School employs this method of backhaul connectivity to bridge 120 miles of California coastline south to Camp Roberts California where much of our experimentation is conducted. The 802.16 Redline OFDM backbone provides 18 Mbps of transmission bandwidth. The Naval Postgraduate School backbone uses 4 foot parabolic dish antennas to bridge the 120 mile gap between Camp Roberts and Monterey in 5 hops. The longest single hop is 62 kilometers.

Temporary backhaul similar to that in use by NPS could be constructed using the roof tops of tall buildings and any communications towers that remain standing on or near a line toward an active ISP. Once connected to the Internet infrastructure the backbone could remain for as long as required or augmented to provide increased bandwidth as required until indigenous infrastructure can be restored.

2. Hardware Requirements

For the above network configurations Redline AN-50e 802.16 OFDM radios are required at the end points of all the nodes. To maximize the utility of the AN-50 a standard 10/100 Ethernet switch can be plugged directly into the AN-50, using a standard CAT-5 crossover cable to provide connectivity to multiple PCs or other networked devices. AN-50 transceivers are connected to the radio base station by standard RG6 coaxial cable like that used for digital television. Using RG6 cable, the base station can be placed up to 500 feet from the antenna giving a wide range of flexibility in antenna placement The type length, and throughput of the desired link will determine the type, of antenna used.

For applications where a backbone is to be established, two AN-50 radios are used at each relay point. The data flows into a relay point from an AN-50 downstream, into the first radio in the relay point where it is then directly transferred to the second AN-50 for relay to the next node.

3. Power Requirements

The AN-50 is configured to use either 120 volts ac or 28 volts dc. While the AN-50 can easily be powered by 5590 or 390 military batteries, the peripheral gear such as switches and 802.11 access points require 120 volts ac. Since most of the peripherals will require 120 volts, a simple solution to provide power, where none or little is available, is the use of readily available 120 volt sine wave inverters and standard marine deep cycle 12 volt batteries. The AN-50s and other peripherals consume a modest amount of power making this a viable solution for even extended operating periods. As situations permit ultra small gas generators, like those built by Honda, can be added to the various sites to provide direct power to the devices or used in combination with a battery charger to maintain the battery's charge.

4. Software Requirements

There are no specific software requirements to use the AN-50e. Any computer equipped with a Microsoft Windows operating system and a standard CAT-5 interface will be capable of connecting to the AN-50.

F. KATRINA DISASTER RELIEF IMPLEMENTATION

On Tuesday September 6, 2005 a Naval Post Graduate School Faculty members Alex Bordetsky and Eugene Bourakov accompanied by PHD and Masters students CDR John Looney and Maria Vetter respectively reported to Naval Air Station Pensacola FL. The mission of the NPS team was two fold. First, the team was to assist Naval disaster relief forces establish a collaborative virtual working environment in Groove Virtual Office. The second mission was to bring the necessary equipment and be prepared to rapidly establish a network foot print in the disaster area if required.

The need and opportunity to establish and provide a network foot print soon arose in Pascagoula MS where mortuary and salvage divers from the United States, Canada, and France were without network connectivity at there bases of operations in Naval Air Station Pascagoula MS. The NMCI network that had serviced the bases was severed by storm action during hurricane Katrina.

The nearest operational connection point was onboard USS SAN ANTONIO LPD 17 moored nearly 2 miles away. A link to SAN ANTONIO was established using Redline AN-50e OFDM radios and one foot parabolic antennas (Figure 14). The stable link provided a constant 12 Mbps of throughput from the diver's base of operations to SAN ANTONIO. From SAN ANTONIO internet connectivity was provided by SATCOM.

Figure 14. OFDM link to USS SAN ANTONIO LPD 17

Additionally an ITT mesh network was established through an ITT access point to provide wireless connectivity to multiple laptop computers throughout the dive team head quarters area. The ITT mesh enabled laptops were able to access the network individually or where necessary extend the network through the mesh to points that required connectivity in the immediate area. After installation, the network continued to operate without support for over 10 days through the time of this writing. The rapid establishment of this network was a real world proof of concept in the viability and utility of portable network extension to support military operations other than war.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. TNT 05-3 SHIPBOARDING PROOF OF CONCEPT AND FIELD TRIAL

Sea control and rapid extension of the network at sea provides unique challenges for the Tactical Network Topology (TNT). Long distances, harsh environment, limited power resources, and large amounts of electromagnetic interference are just a few of the obstacles to be overcome. During TNT 05-3 and TNT 05-4 experimentation the Redline AN-50M portable 802.16 OFDM broadband radio has become the primary backhaul method for Visit Board Search and Seizure operations. The use of an 802.16 backhaul stems from the limited ability of the 802.11 wireless backhaul attempted in earlier experimentation. While not a failure, the 802.11 link had a great deal of difficulty overcoming the increased range and radio frequency interference that is part of the maritime operating domain. The following data and operational information is a result of the ship boarding proof of concept experiment during TNT 05-3.

A. TNT EXPERIMENT 05-3

Experiment TNT 05-3 was the first attempt at using portable 802.16 OFDM to replace the 802.11 backhaul used in previous ship boarding experimentation. The AN-50M prototype was unavailable for the experiment so a standard AN-50e configured to use 28 volts DC was mounted to a backpack frame and used as a surrogate. The surrogate's use and performance was not a problem in this instance because the internal components of the AN-50e and the AN-50M are virtually identical. The only major difference was the power input requirement; the AN-50e requires 28 volts DC and the AN-50M requires 12 volts DC. The TNT 05-3 ship boarding scenario onboard the USCGC HAWKSBILL was designed to be a proof concept utilizing 802.16 to backhaul data from a rapidly deployed 802.3 shipboard Ethernet and a LLNL ultra wideband network.

B. EXPERIMENT ASSUMPTIONS

Future maritime and port security network centric interdiction operations will require the use of broadband communications. The broadband backhaul will be mated

with a robust jam and interference resistant RF technology capable of transmitting mission critical data through ships superstructures and cargo containers efficiently and effectively. Mission critical data provided by numerous assets will enhance rapid detection and capture of high interest cargo or persons. Boarding team assets could include video capture devices (allowing facial recognition, and cargo identification), audio communications, portable radiation detection and classification, digital document acquisition, transfer and archiving. All network and detection assets must be ruggedized for marine environments and highly portable for rapid deployment. An integrated network for all assets and expert services reach-back is essential for providing situational awareness, a common operational picture, and collaborative behavior. In the near future this will also permit autonomous, collaborative behavior of large numbers of boarding teams utilizing highly skilled distant technical support to enhance mission capabilities.

C. BASIC EXPERIMENTAL REQUIREMENTS TO BE EXAMINED

1. Land or Ship-Based OFDM Base Station

The ship or land based 802.16 OFDM base station will ideally be a point-to-multi-point 802.16 OFDM node. In the TNT experiment, due to limited participating nodes, 802.16 OFDM was configured to the point-to-point mode.

2. Portable OFDM Remote Station

The portable 802.16 OFDM node requires a battery life of several hours with provision for easy change-out in the field. The remote node must be hardened to resist impact and environmental damage. Mobile back-haul 802.16 OFDM must support the establishment of a rapidly deployable LAN .

3. Data Transport to 802.16 OFDM Remote Node

Data transport from within a boarded vessel to the 802.16 OFDM remote station provides numerous challenges to wireless communications including various sources of inference (radar, shipboard electrical service, and penetration of multiple levels of steel decking or walled cargo containers). Lawrence Livermore National Laboratory (LLNL) Ultra-Wideband technology is being provided as a possible solution to this problem. Ultra-Wideband RF links could be used in areas where a simple rapidly deployed

Ethernet LAN is not feasible. Other solutions for boarding team LANs may include low frequency RF radio modems or single use disposable wired networks.

4. IST GN5 radiation detection concept device ergonomics

Crucial to rapid detection and threat assessment of radiation hazardous material is a portable detection unit with the capability to rapidly detect, provide initial identification, and quickly relay information via the 802.16 OFDM back-haul to a remote location for expert analysis. Currently Innovative Survivability Technologies (IST) is developing a scaled-down version of their larger static vehicle radiation detection and identification sensor system. The new sensor will be man portable, weigh less than 15 lbs, and be sufficiently ruggedized for boarding team use.

D. TNT 05-3 EXPERIMENTAL OBJECTIVES

The TNT 05-3 boarding experiment was intended as a proof of concept trial. The goal of the boarding experiment focused on three aspects. The first critical milestone was the use of portable 802.16 OFDM technology to establish a stable backhaul link. Second, the boarding party attempted to seamlessly integrate 3 networks to provide a common operating picture. If successful, the network integration of Ultra-Wideband through a rapidly formed 802.3 Ethernet LAN and backhaul by 802.16 OFDM will be the first of its kind in TNT experimentation. The third focus of this proof of concept was ergonomic testing of IST's GN-5 radiation detection and classification unit.

E. EXPERIMENTATION AND DEMONSTRATION OF TECHNOLOGY

The TNT 05-3 ship boarding experiment was conducted on the afternoon of May 18 2005. LLNL, NPS, and IST research teams boarded the Coast Guard Cutter HAWKSBILL and proceeded to carry out the proof of concept and field trial experimentation throughout the afternoon.

1. 802.16 OFDM Base and Remote Station Performance

The NPS AN-50M research team established an 802.16 link between HAWKSBILL and the research vessel CYPRESS SEA using a Redline AN-50e configured as a surrogate AN-50M. The antenna configuration used was two 16-inch omni-directional antennas providing 9 db of gain on the respective ends of the link. The

Cypress Sea research vessel acted as a relay point between the boarded vessel (USCGC HAWKSBILL) and the Del Monte Beach Lab.

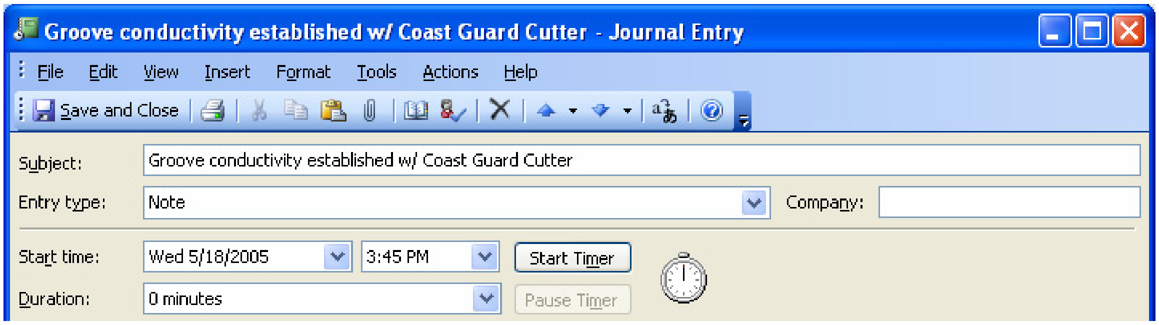


Figure 15. 802.16 connectivity established between HAWKSBILL and the TOC

The 802.16 data link between HAWKSBILL and Cypress Sea was initially unstable due to a non-line-of-sight status between HAWKSBILL and CYPRESS SEA, driven by CYPRESS SEA's commitment to a concurrent experiment. The OFDM data link was stabilized once CYPRESS SEA took a position in line-of-sight at approximately 1000 meters per the experiment guidelines (Figure 15). From the point of stabilization the OFDM link performance was excellent, providing on-average 1.5 to 2.0 Mbps throughput between HAWKSBILL and CYPRESS SEA. Battery life using two standard military Mil-390 nickel medal hydride rechargeable batteries was in excess of 4 hours. The connectivity and throughput provided by the AN-50 Man-Pak was more that sufficient for the voice, video and data transfer required by the boarding team (Figure 15).

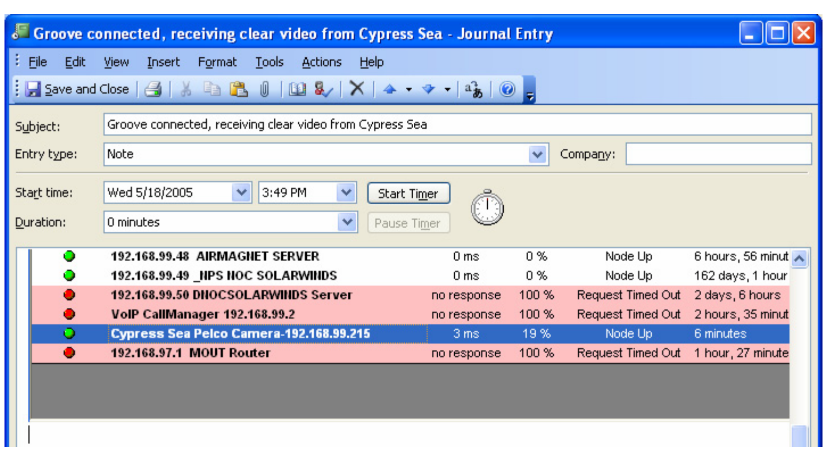


Figure 16. Video connection from HAWKSBILL established

2. LLNL Ultra-Wideband RF Technology Field Trials

The Lawrence Livermore National Laboratory set up and tested internal shipboard communications using their Ultra-wideband technology. The initial setup of ultra-wideband (UWB) on the HAWKSBILL bridge was unstable and provided limited connectivity. After analyzing and repositioning the UWB antenna and receiver about 8 ft from the original location a stable UWB link was established that allowed data transfer from the vessel's engine room two decks below the receiver (Figure 17). Following successful establishment of an UWB link, a simulated radioactive material histogram was sent from the UWB network across the boarding team 802.3 Ethernet LAN to the 802.16 OFDM backhaul link and on to LLNL collaborative partners for technical analysis. The successful transmission of the test file established that an UWB RF link, rapidly established Ethernet LAN, and 802.16 OFDM could work in concert to provide near-real-time situational awareness and collaboration for military and law enforcement maritime security operations.

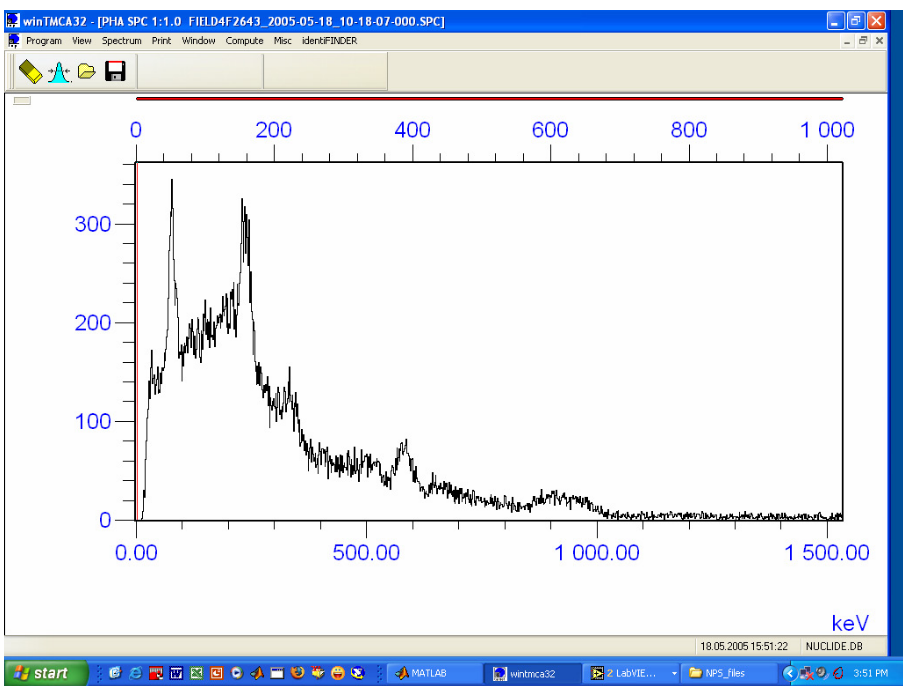


Figure 17. Radiation detection histogram test file

3. IST Portable Radiation Detection Development

The Innovative Survivable Technologies team conducted initial ergonomic fit and feel experimentation as part of an initial phase development in partnership with LLNL of

a man portable radiation detection and classification device for shipboard use. Utilizing Coast Guard crew members of HAKSBILL the GN5 concept device was wear-tested for fit and feel. The initial testing provided positive feedback that the design concept for the radiation detection device was both man-portable and ergonomically functional in the shipboard environment.

F. TNT 05-3 CONCLUSIONS

The TNT-05-3 ship boarding was a highly successful follow-on to the previous ship boarding experiments. As a further extension into the joint NPS and LLNL maritime defense studies for home land security, the use of a joint collaborative UWB, Ethernet, and 802.16 OFDM network was proof of viability for further research. Future boarding experiments should continue to employ the highly successful 802.16 OFDM back-haul technology. 802.16 OFDM exhibited excellent throughput capabilities at extended ranges, combined with low latency and resistance to interference. The 802.16 OFDM link averaged 1.5 to 2.0 Mbps throughput at a backhaul distance of 1000 yards. The link was established using two 9 dBi omni directional antennas.

LLNL ultra-wideband technology performed well after some initial instability. Ultra wideband appears to be well on track to provide a solution to wireless communications in harsh transmission environments. In addition to UWB, further research into the use of low frequency RF and disposable wired networks will also be advantageous to future ship board networking experimentation. The use of small directional antennas for the 802.16 OFDM AN-50M to enhance data link stability and range should also be pursued in follow-on experimentation.

VII. TNT 05-4 VBSS EXPERT SERVICES COLLABORATION SCENARIO BASED EXPERIMENT

As a follow on the TNT 05-3 proof of concept, TNT 05-4 called for UWB and portable 802.16 OFDM to be incorporated into the TNT scenario driven experimentation. The goal of the ship boarding was to test the applicability of using UWB and portable OFDM to facilitate a network allowing expert service reach-back for radiation source analysis by LLNL and biometrics identification support from the National Biometrics Fusion Center.

A. SCENARIO

The Naval Postgraduate School Network Operations Center receives TACSAT ELINT that an inbound cargo vessel may be carrying radioactive material onboard. Since there are numerous commercial uses for certain radioactive sources, positive identification of the source in a short time frame with minimal disruption to the surrounding cargo is imperative. Further human intelligence indicates some of the cargo ship crew members may be terrorist suspects posing as crewmen. Support from the National Biometric Fusion Center must be used to quickly and accurately discriminate between actual crew and terrorist suspects. Having received a situational briefing, the NPS and LLNL boarding team members move to board the suspect vessel and establish a collaborative network.

B. BASIC REQUIREMENTS

1. Land or ship based OFDM base station.
2. Portable OFDM remote station capable of several hours of sustained battery operations.
3. Effective data transport to mobile OFDM node from boarding team assets possibly accomplished through Ultra-Wideband RF technology or low frequency radio network technology.

C. DISCOVERY AND DEMONSTRATION TECHNOLOGIES

1. Mobile man-portable OFDM backhaul link to TNT test-bed
2. Ultra-Wideband interface and data transport to OFDM node from boarding team.
3. Electronic biometrics gathering and uplink to Biometric Fusion center in West Virginia
4. Potable radiation detection and identification via live link between LLNL and boarding team using radiation detection device.
5. VPN reach-back to various TNT collaborative partners.

D. CAPABILITIES/ASSETS

1. All ultra-wideband tactical equipment connected to 802.16/OFDM network
2. Assets: NOC, Beach Lab, CYPRESS SEA research vessel, and USCGC HAWKSBILL, portable radiation detection and Biometrics equipment, VPN reach-back to all required Collaborative partners.

E. APPLICATIONS

1. Capabilities: Stream audio, video and data from USCGC HAWKSBILL through man-pack OFDM and ultra-wideband.
2. Groove Networks collaboration Software

F. EXPERIMENT VARIABLES

State Variables

1. Time and space variations of network node locations
2. Distance of portable OFDM node from CYPRESS SEA, distance of ultra-wideband sensors from man-pack.

Environmental Variables

1. Weather
2. Wireless traffic (UWB, non 802.16, ambient RF interference)

G. MEASURES OF PERFORMANCE

Network Performance

1. Ability to establish mobile 802.16/OFDM link.
2. Throughput as function of time on OFDM
3. Availability of uplink and downlink

Collaborative Service Reach-back Performance

1. Ability to provide biometric data and radiation detection data via VPN reach-back to Biometric Fusion Center and LLNL.
2. Access time for remote sites (Operational)
3. Feasibility of applications
4. Presentation of sensor sites in SA

Collaborative Performance

1. Latency of sync with all sites (out band coordination)
2. Frequency of messaging and ACK (by NOCWO log)
3. Reliability and quality of asset video (remote site observation)

H. 23 AUG 2005 SCHEDULE OF EVENTS

To be tested is the Man-Pack OFDM backhaul link, LLNL Ultra-Wideband (UWB) interface and portable biometrics gathering equipment.

Network availability is a function of the 802.16/OFDM backbone from the Beach Lab, to the Man-Pack 802.16/OFDM radio and the links between the Biometrics, UWB, video, and Radiation detection devices.

Network availability and capability will then be tested throughout the boarding evolution conducted on USCGC HAWKSBILL. Network availability will be tested to the most remote node (UWB) and Man-Pack 802.16/OFDM throughout the boarding evolution to determine the effects of bulkhead and deck penetration on UWB and backhaul distance from HAWKSBILL to CYPRESS SEA effect on the OFDM link.

1. Event 1

NPS Man-Pack, LLNL UWB, Biometrics Fusion Team, and IST development teams will board USCGC HAWKSBILL. UWB, Boarding Officer, and Radiation Detection, and Biometrics teams will establish and stabilize boarding team LAN on target vessel. Man-Pack Operator will establish OFDM link to CYPRESS SEA and send audio/video link via Groove workspace to collaborative partners.

2. Event 2

Biometrics fusion team will establish connectivity and begin gathering and processing biometrics from suspect vessel crew via reach-back to the Biometrics Fusion Center provided by TNT test-bed.

3. Event 3

After OFDM link is established LLNL team will interface UWB with the OFDM link and stream video back to the NOC.

4. Event 4

LLNL team will use portable radiation detector to evaluate potential cargo of interest onboard USCGC HAWKSBILL. Radiation data will be streamed through the OFDM backbone and associated VPN portal to LLNL remote technical assistance engineers for further identification expert analysis.

5. Event 5

While boarding teams are aboard HAWKSBILL the IST development team will observe and document ergonomic and functional requirements for future under-development portable radiation detection and source identification units.

I. SCENARIO PERFORMANCE AND EFFECTIVENESS

On August 23, 2005 the NPS boarding team, with member support from LLNL radiation detection and ultra-wideband personnel and National Biometrics Fusion Center personnel, boarded the suspect vessel USCGC HAWKSBILL. The boarding was made in response to an ELINT and HUMINT notification that the vessel was carrying illicit crew and cargo.

1. Network Performance

The boarding team 802.3 Ethernet LAN was quickly established following team members arriving onboard HAWKSBILL. Total setup time for the Ethernet LAN was less than 10 minutes with connectivity to Boarding officer laptop computer on the ship's bridge, LLNL laptop computer on the main deck, and the Biometric Fusion Center computer on the focsale (bow of the vessel). Shortly after the 802.3 LAN was established, Groove connectivity on the local network was established and synchronized.

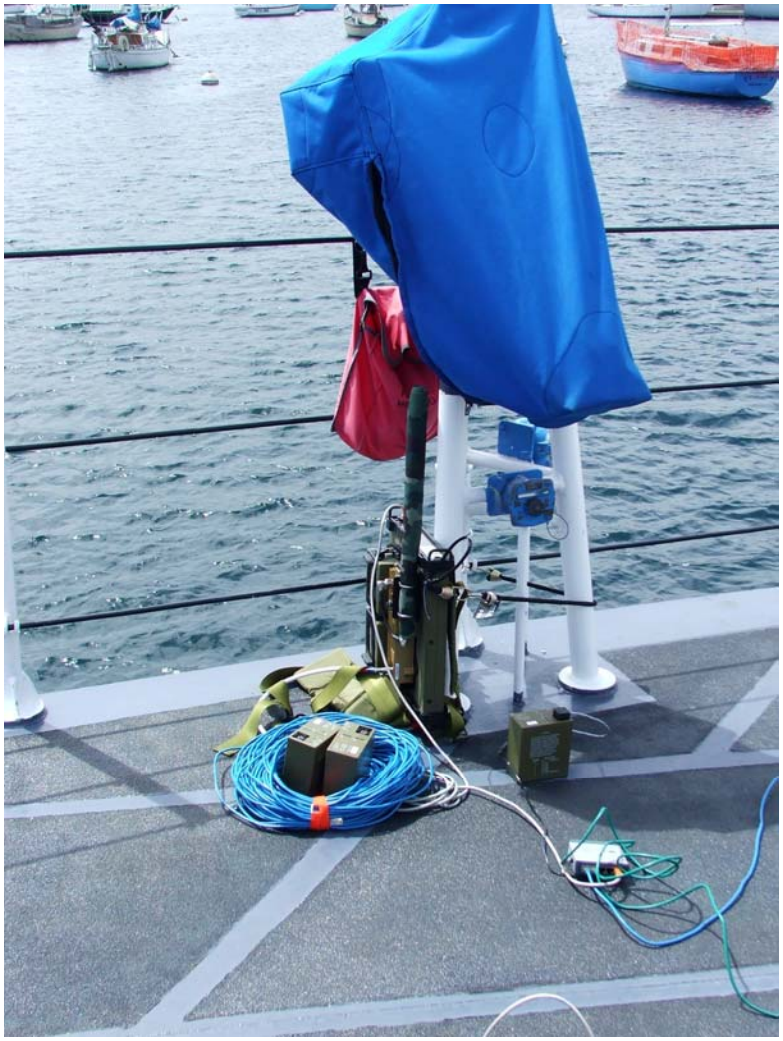


Figure 18. AN-50M and battery powered Linksys switch provide boarding team nodes with backhaul and connectivity off the suspect vessel

Following a successful operation test of the boarding team LAN, the 802.16 OFDM link was initialized and connected between HAWKSBILL and the Del Monte Beach Lab approximately 2000 yards away. The link was not visual line-of-sight due to some slight obstruction by foliage near the Del Monte Beach Lab. The AN-50M was simply placed upright against a 50 caliber machine gun mount for stability (Figure 18). Although the placement of the AN-50M was not optimal for antenna and Fresnel zone clearance, it was indicative how the device would most likely be positioned in an operational environment. The link remained stable with a receive signal strength of -74 to -78 dBm and periodically dipping to -80 to -83 dBm. As seen previously in chapter 3 table 1, the calculated receive signal strength is approximately -72 dBm. The wider

fluctuations noted in the actual (Figure 19) link are most likely due to the noted foliage obstructions and interference caused by the ship's structure around the AN-50M.

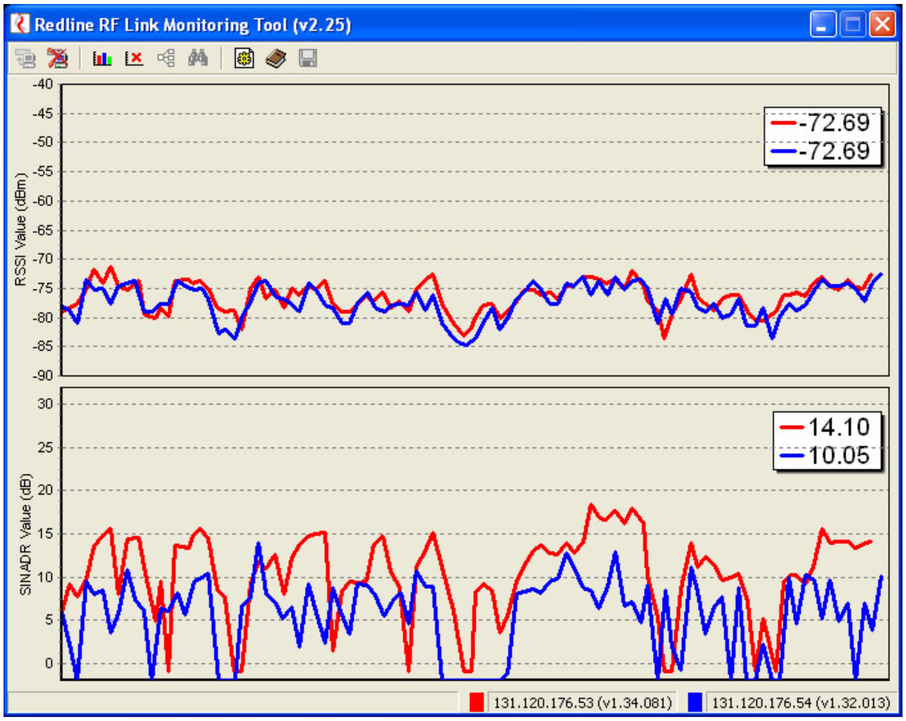


Figure 19. Received signal strength of AN-50M link to Del Monte Beach Lab in RFmonitor

Once established the OFDM link and network connectivity remained active and stable for the entire 5 hour boarding evolution. The link was more than adequate to stream video and voice over IP. 11:00am was the high point of data transfer where the link was sending and receiving at a rate of just under 1.0 Mbps. The Solar Winds monitoring tool only displays a passive view of the network throughput based on an actual network load. The 11:00 am time frame network health as viewed in Solar Winds shows high throughput (800 Kbps), with low response time (< 4 ms) and packet loss percentage with some spikes but averaging 60-70 percent (Figures 20 and 21). The listed indicators are representative of a healthy and stable link.

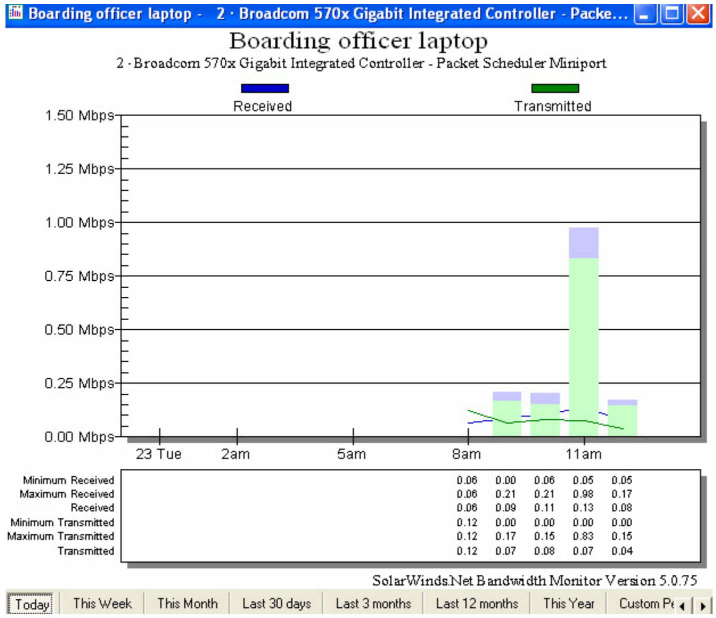


Figure 20. AN-50 throughput over time

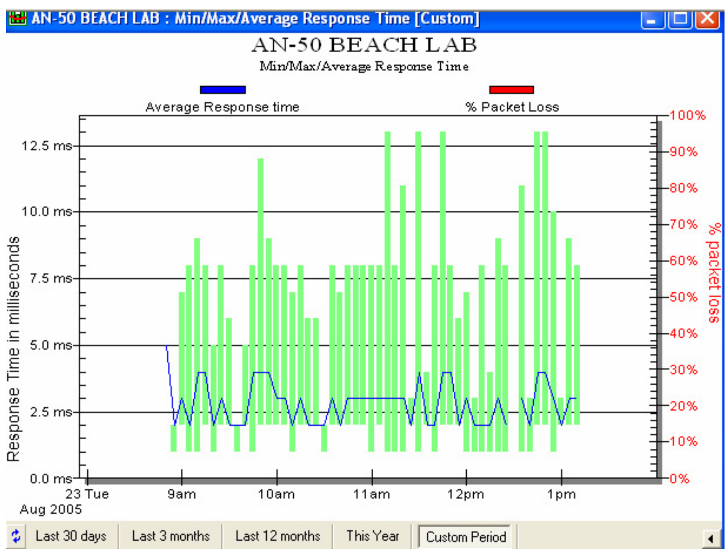


Figure 21. 802.16 OFDM link average response time and packet loss over time

The LLNL ultra W\wideband network performed well, providing a data link for GN5 radiation detection capture files. The UWB link was established between the ship's engine room and the main deck. Radiation source spectrum captures were made of a container that was detected to have a radiation signature presence. The UWB network backhauled source histograms directly to a networked LLNL laptop. From the networked

laptop files were transmitted via the Groove Virtual work space for analysis by LLNL physicists.

2. Collaborative Service Reach-back

The self synchronizing collaborative workspace provided by Groove worked as planned to bring remote expert services in the boarding team's tool set. Groove facilitated voice and text communication between all members of the virtual boarding party and the physical boarding part. VPN connectivity between LLNL and The Biometrics Fusion Center was created to provide a secure working environment while taking advantage of the established internet connectivity at the Beach Lab and Naval Postgraduate School NOC. The VPN connectivity allowed all the participants to operate in the Naval Postgraduate School 131.120.x.x address space. Latency across the entire shared work space was negligible.

Both LLNL and The Biometric Fusion Center were able to receive and open posted files in less that two minutes to begin analysis once they were posted to Groove onboard HAWKSBILL. The "expert services" provided at LLNL quickly determined that there was a need for additional data capture of longer length and different angles of approach. The request was transmitted by a Groove text message and taken for action quickly with minimal waste of time.

Three low level radioactive sources were used in the radiation detection experiment. A thoriated lens as a representative industrial source, an Am-241 source #300899 of ~8uCi, and a Cf-252 source #120365 of ~4uCi were all used in a small cardboard box container and planted without the knowledge of the GN5 operator. The thoriated lens was used as a distraction to hopefully mask the other two less common more eye raising sources. The GN5 easily detected the presence of the radioactive sources (Figure 21). When analyzed by LLNL it was apparent that more than a standard source was present. The analysis led the boarding officer to recommend that the vessel by quarantined for further inspection. (Dougan, 2005)

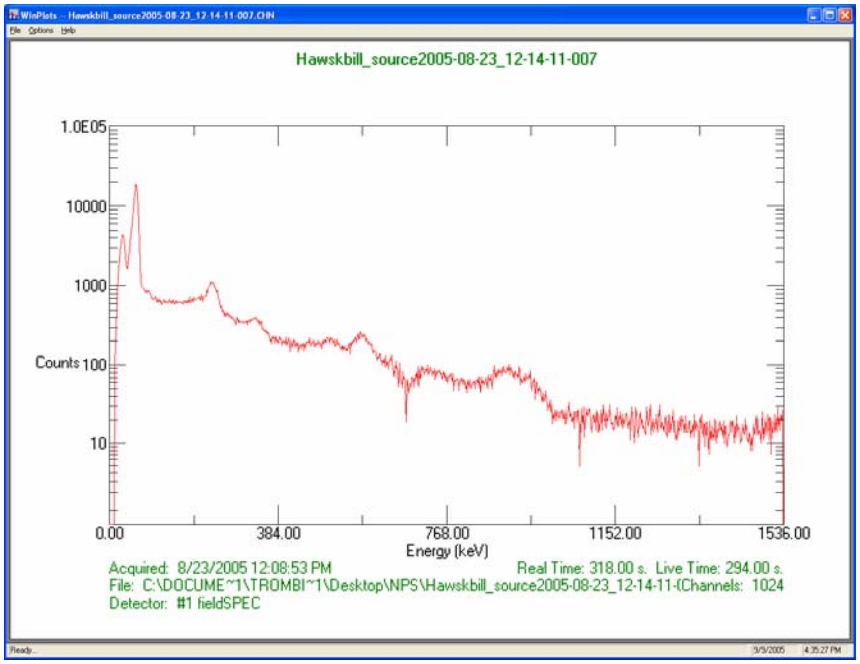


Figure 22. GN5 live source detection histogram (Dougan, 2005)

On the focsal the Biometric gathering team took digital "ten prints" of the crew to compare to know criminal and latent prints lifted from terror and crime scenes. Although the data base being used for the experiment was a simulation, it was configured identical to the actual data bases and used the same comparison algorithms. Know "simulated" bad finger prints were submitted to the database before the experiment and were unknown to the operators except that one of the numerous sets of prints that where taken should be a match. The system correctly identified the same bad prints when submitted using two different aliases with a group of 5 other prints. Total turn around time to positive or negative identification on submitted "ten print" cards was 15 to 20 minutes.

3. Collaborative performance

There were no problems with collaborative performance of tools during the ship boarding evolution. Most operational coordination was handled by voice over IP to the various nodes. Group chat and individual text messaging was also extensive. The ability to text message and communicate in a voice over IP mode essentially mitigated a need to communicate in other out-of-band modes such as cell phone or two-way radio. The only situational awareness tool (SA) worked well to provide limited positional data and alerts to large events. The only tool that had intermittent problems was the video conference

provided by the Naval Postgraduate School ISGIANT/VC1 server. It was unknown if the problem was based on link performance or software interface and more testing will be required to make that determination.

J. EXPERIMENT CONCLUSIONS

The TNT 05-4 experimentation on shipboard VBSS operations, collaborative reach-back, ultra-wideband wireless RF, and 802.16 OFDM networking was a success. The scenario observed by numerous guests including Jim Fletcher from the US Coast Guard Office of Research and Development, California Highway Patrol, and other state and local first responders was echoed by most as an "impressive display of technological capabilities". The 802.16 backhaul link again performed well, providing over 800 Kbps of throughput over a 2000 yard link. The 200 yard link was established using a 9 dBi omni directional antenna on the AN-50M and a 60 degree 16 dBi sector antenna at the Del Monte Beach Lab.

The ample bandwidth provided by the AN-50M easily allowed VPN reach-back to the expert resource and capabilities of LLNL and The Biometrics Fusion Center. In addition to the virtual boarding team formed by the collaborative workspace, everyone on the network had near-real-time access to the resources of the world wide web. With proper planning and installation of a simple shared workspace like Groove to other national, state, and local resources, the reach-back capability of the rapidly extendable network could leverage a greater and greater knowledge and resource base.

VIII CONCLUSIONS AND RECOMMENDATIONS

A. CONCLUSIONS

1. Broadband Wireless Network Extension CONOPS

The concept of rapidly extensible wireless broadband is crucial to the future of network centric warfare and network centric law enforcement. The maritime threat environment is changing rapidly. In order to keep pace with changes, technology must be leveraged to the fullest extent possible. The AN-50M 802.16 OFDM radio is proof positive that a proven technology like the Redline AN-50e OFDM radio can be modified to construct rapidly deployable mobile networks.

The broadband wireless extension offered by the AN-50M has shown that a single digital back-haul methodology cannot only replace existing voice communications, it can also transfer data, video and more. Captured data can be quickly archived for future reference or pushed in near real-time to collaborative partners providing expert service analysis. The common operational picture provided by these tactical networks is what will be required to operate on a joint basis with not only indigenous United States military and law enforcement but also world wide partners in maritime security.

2. Ultra-Wideband Technology

The LLNL ultra-wideband technology has been consistently increasing in capability and allowing wireless links to overcome boundries that push the wireless envelope. During both the proof of concept TNT 05-3 and scenario driven TNT 05-4, ultra-wideband has demonstrated that it can provide a viable backhaul link from isolated areas through difficult RF propagation channels. Given the operating environment of merchant cargo and container ships ultra-wideband provides possibly one of the only methods available to establish a wireless data link.

3. Expert Services

The use of expert services for the scenario driven TNT 05-4 experiment was the key to success. The expert service reach-back portion of the experiment was a continued thread on the proof of concept of leveraging network centric operations. In the current field methodology, capture and identification of criminal suspects that are linked to latent finger prints takes days or even weeks. Finger prints are captured using ink and paper

then mailed to a location for analysis. Paper cards and long lag time is not a problem for a captive suspect, however trying to intercept illicit passengers and crew in the merchant shipping environment has a far shorter time constraint. The Biometric Fusion Center database and processing power combined with a collaborative tool such as Groove Virtual Office essentially allows the rapid biometrics analysis anywhere a network link can be established. The same type of service is provided by LLNL for radioactive source analysis. When so much rides on being correct nearly 100 percent of the time in port security and maritime interdiction operations dealing with terrorism and weapons of mass destruction, it only makes good sense to bring every technology weapon to bear that will reduce the chance error.

B. RECOMMENDATIONS

1. AN-50M

The AN-50M is essentially a portable version of the rack- mounted AN-50e. The AN-50 performs well but is useless to a human operator as a stand alone node. In order to configure and operate the AN-50 a minimum of a laptop and CAT-5 patch cable are required. For any extensive use of the broadband capabilities provided by the AN-50 a switch is required to connect multiple devices. The additional gear required for general operation increases weight and also requires separate power supplies to function.

To increase portability and reduce equipment load a "smart" AN-50 that incorporates a CPU, touch plasma screen and 5 port Ethernet switch should be a focus of development.

In addition to the smart AN-50M, the 802.16 OFDM wave form and PHY layer could be examined for potentially shifting the frequency out of the 5.8 GHz band. Specifically a shift to a lower frequency may be desirable to facilitate better penetration and range.

2. Low Frequency Radio Modems

Low frequency point to multi-point radio modems such as those built by Freewave Inc, could be used in a complimentary application to the LLNL ultra-wideband. The Freewave or other radio modems operating in the military band near 133 MHz could

provide excellent low bandwidth backhaul solutions. Low frequency offers increased open country range, especially to an air node. In a ship boarding environment the 133 MHz RF should exhibit much better penetration through hardened structures.

3. Disposable Wired Networks

During all of the CENETIX experimentation, as would be expected, wired networks are typically the most reliable links. A rapidly deployable wired network that is based on a light weight disposable medium has potential for tactical deployment. A disposable network could leverage the reliability of wire and known mature protocols like 802.3 Ethernet. Furthermore wireless protocols could provide an answer to excessive line-loss and impedance in small disposable wired networks by using the wire as little more than a wave guide.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Adlawan, B. 2005. *GN5 hand held gama-neutron detector identifier*

Anderson, M. C., & Winterstine, B. 2004. *A network-centric approach to maritime domain awareness*. Last Accessed July 2005

Bach, E. J., & Fickel, M. G. 2004. An analysis of the Feasibility and Applicability of IEEE 802.X Wireless Mesh Networks Within the Global Information Grid. (Masters Thesis, Naval Postgraduate School, Monterey, CA)

Blazevich, R. J. 2004. Wireless, Long Haul, Multi-Path Networking: Transforming Fleet Tactical Network Operations With Rapidly Deployable, Composable, Adaptive, Environments. (Masters Thesis, Naval Postgraduate School, Monterey, CA)

Dougan, A. 2005. *Email: Subject: Sources From: adougan@llnl.Gov*

Eklund, C., Rodger B. Marks, & Kenneth L. Stanwood. 2002. *IEEE Standard 802.16: A Technical Overview of the WirelessMAN Air Interface for Broadband Wireless Access.* IEEE. Last Accessed September 2005

Herzig, J. F. 2005. An analysis of the feasibility of implementing ultra wideband and mesh and mesh network technology in military operations. (Masters Thesis, Naval Postgraduate School)

HSW-1. *How stuff works - ethernet.* Retrieved 2005, Last Accessed September, 13, 2005 from http://computer.howstuffworks.com/ethernet1.htm

HSW-2. *How stuff works.* Retrieved 2005, Last Accessed September, 13, 2005 from http://computer.howstuffworks.com/wireless-network.htm

Kathein Inc. 2004. *Engineering Reference – Equasions*.pdf

Klopson, J. E., & Burdian, S. V. 2005. Collaborative applications used in a wireless environment at sea for coast guard law enforcement and homeland security missions. (Masters Thesis, Naval Postgraduate School, Monterey California)

Moltzan, T. 2005. Design and analysis of a wireless telemetry system utilizing IEEE 802.16.

Networks, Groove. 2004. *Whats New in Groove Virtual Office*

Redline Communications. 2005. *AN-50e Product Data Sheet*

Redline Communications. 2003. *Second Generation High-Capacity Broadband Wireless Solutions*

Redline Communications. 2003. *Advantages of Broadband Fixed Wireless Systems Over 802.11 LANs*

Rennie, G. 2003. Portable radiation detector provides laboratory precision in the field. *Science & Technology Review,* Last Accessed September, 12, 2005

Suitor, Kevin F. R. 2004. *From "a" to "e": The 802.16 Standard Evolution*

Suitor, Kevin F. R. 2004. *What WiMAX Forum Certified™ will Bring to WiFi™*

TBW. 2005. *TeraBeam wireless.* Retrieved 2005, Last Accessed September, 13, 2005 from http://www.terabeam.com/support/calculations/fresnel-zone.php#meters

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Dan Boger
   Naval Postgraduate School
   Monterey, CA

4. Alexander Bordetsky
   Naval Postgraduate School
   Monterey, CA

5. David Netzer
   Naval Postgraduate School
   Monterey, CA

6. Christopher Marvin
   Naval Postgraduate School
   Monterey, CA